ANEXO. ACUERDO DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

CLÁUSULAS

PRIMERA – DEFINICIONES: Para efectos del presente Acuerdo, se entenderá por:

1) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales, el cual debe otorgarse a más tardar al momento de recolectar los datos a tratar.
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.
3) Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento.
4) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

   Al respecto la Corte Constitucional mediante sentencia C-748 de 2011 señaló lo siguiente: *la jurisprudencia constitucional ha precisado que las características de los datos personales –en oposición a los impersonales- son las siguientes: "i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación."*
5) Datos sensibles: 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.
6) 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, para el caso en concreto será: CONTRATISTA SELECCIONADO.
7) 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, para el caso en concreto: EMPRESA DE TRANSPORTE MASIVO DEL VALLE DE ABURRÁ LIMITADA – METRO DE MEDELLÍN LTDA.
8) Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

9) Transmisión: Tratamiento de Datos Personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia, con el objeto de permitir a EL RESPONSABLE y a EL ENCARGADO realizar el Tratamiento de los Datos Personales.
10) Tratamiento de datos personales: Será cualquier operación o conjunto de operaciones consistentes en la recolección, circulación, organización, almacenamiento, consulta, uso, acceso, actualización, diseminación, bloqueo, eliminación, supresión o destrucción de los datos personales.

SEGUNDA - OBJETO: En virtud del presente Acuerdo, las Partes buscan regular las condiciones y la forma como se dará cumplimiento al Régimen de Protección de Datos Personales tanto por parte de quien actúa como **RESPONSABLE** de la Base de Datos, como de quien asume la posición de **ENCARGADO**.

En atención y en desarrollo del Contrato No. XXXXX, **EL RESPONSABLE** Transmitirá a **EL ENCARGADO,** datos personales de personas que pertenecen a la Base de Datos

- Administración del Talento Humano – Virtual (Servidores históricos y actuales, aprendices históricos y actuales, practicantes históricos y actuales, familiares).
- Gestión predial – Virtual (propietarios a quienes se les han realizado pagos).
- Procesos contractuales – Virtual (contratistas actuales e históricos).
- Usuarios Cívica – Virtual.
- Gestión Urbana – Virtual (Clientes históricos y actuales, clientes venta de predios).
- Hechos relevantes – Virtual.
- Procesos judiciales y extrajudiciales (personas a quienes se les han realizado pagos).

✓ Finalidad de la Transmisión: Permitir que **EL ENCARGADO** trate datos personales por cuenta de **EL RESPONSABLE**, exclusivamente para ejecutar las actividades técnicas, funcionales y operativas necesarias para la conversión, migración, configuración, integración, pruebas, estabilización, soporte y documentación de la plataforma ERP SAP ECC 6.0 EHP8 a SAP S/4HANA bajo modalidad RISE en AWS.

✓ Datos a Transmitir: Datos públicos como nombre, tipo de documento, número de documento, fecha de nacimiento, lugar de nacimiento, etc.; Datos semiprivados, como teléfono, dirección, correo electrónico, datos salariales, datos financieros, datos de nómina, , número de Tarjeta Cívica, etc; Datos de menores de edad (familiares de servidores, protagonistas de hechos relevantes, usuarios cívica, etc;

Así mismo, **EL ENCARGADO** realizará los siguientes Tratamientos:

✓ Podrá USAR los datos personales a los que tenga acceso única y exclusivamente para analizar, convertir, migrar, configurar, ajustar, validar, probar, estabilizar, soportar y documentar los componentes, desarrollos, interfaces, roles, perfiles, módulos y procesos necesarios para la transición de SAP ECC 6.0 EHP8 a SAP S/4HANA bajo modalidad RISE en AWS, conforme a las instrucciones de **EL RESPONSABLE**.

PARAGRAFO: El tratamiento de los datos se realizará mientras se mantenga vigente el Contrato mencionado, salvo acuerdo particular en contrario entre las Partes y en ningún caso podrá extralimitarse a las finalidades establecidas por **EL RESPONSABLE** en su Política de Tratamiento de Información y Datos Personales.

TERCERA – ALCANCE: Las Partes han acordado, que las actividades a realizar con la información contenida en la Bases de Datos por parte de **EL ENCARGADO** serán:

a. Análisis técnico, diagnóstico y preparación de los ambientes SAP requeridos para la conversión y migración.

b. Conversión, migración, homologación, validación y carga de datos, estructuras, tablas, configuraciones y datos maestros necesarios para la transición a SAP S/4HANA.

c. Análisis, ajuste, conversión y validación de desarrollos, personalizaciones, códigos, reglas de negocio e integraciones que puedan contener o relacionarse con datos personales.

d. Configuración, actualización y validación de usuarios, roles, perfiles, permisos, flujos de aprobación y reglas de acceso al sistema.

e. Migración, configuración, prueba y validación de interfaces entre SAP y otros sistemas internos o externos de **EL RESPONSABLE**.

f. Implementación, configuración, prueba y validación de módulos o funcionalidades que involucren datos de empleados, usuarios internos, proveedores, contratistas, terceros, pagos, recaudos, cuentas bancarias, inventarios, trazabilidad operativa, reportes o información regulatoria.

g. Ejecución de pruebas técnicas, funcionales, integrales, de regresión, estabilización y salida a producción, procurando el uso de datos anonimizados, enmascarados, ficticios o minimizados cuando sea posible.

h. Atención de incidencias, soporte, acompañamiento, monitoreo y estabilización del sistema durante la ejecución del proyecto.

i. Generación, consulta, revisión y entrega de reportes, logs, evidencias, actas, manuales, documentación técnica, funcional y de usuario que puedan contener datos personales.

j. Transferencia de conocimiento y capacitación a usuarios técnicos, funcionales o finales, únicamente en lo necesario para la administración, operación y soporte del sistema.

k. Conservación temporal, devolución, eliminación o anonimización de la información a la que tenga acceso, una vez cumplida la finalidad del Tratamiento o finalizado el contrato, según las instrucciones de **EL RESPONSABLE**.

CUARTA – TRATAMIENTO DE DATOS PERSONALES: EL ENCARGADO, acepta obligarse en los términos de este Acuerdo, para llevar a cabo el Tratamiento de datos personales de acuerdo con los términos de (i) los principios y normas contenidas en la Ley Aplicable de Protección de Datos Personales, (ii) la Política de

Tratamiento de la información y datos personales de **EL RESPONSABLE**, (iii) Las finalidades de las Base de Datos transmitida.

EL ENCARGADO no podrá transmitir, ni transferir a terceros información que trate en nombre de **EL RESPONSABLE** y en los casos en que sea estrictamente necesaria la realización de una transmisión, la misma deberá derivar de: una autorización o determinación de éste, una subcontratación u obedezca a un mandato expreso de la autoridad de control; todo lo anterior en virtud del principio de confidencialidad.

EL ENCARGADO dará a conocer los datos única y exclusivamente a sus servidores y/o empleados y demás personas que tengan necesidad de conocerla para realizar el Tratamiento de datos personales relacionados con las finalidades a la que se hace referencia en el objeto y alcance del Acuerdo, a quienes se les advertirá sobre el carácter confidencial de la información y se les deberá dar a conocer los términos de este Acuerdo, y quienes deberán aceptar dichos términos antes de tener acceso a la misma.

QUINTA – CONDICIONES DEL USO DE LOS DATOS:

1) **LAS PARTES** garantizan y aceptan el compromiso mutuo de permitir a los Titulares de los datos personales, el ejercicio de los derechos de acceso, conocimiento, revocatoria, rectificación, actualización, supresión de datos personales y cualquier otro derecho reconocido legalmente relacionado con tales datos.
2) La Transmisión de los datos personales se realizará a través de las herramientas seguras que **LAS PARTES** establezcan para estos fines.
3) El tratamiento de los datos se deberá realizar garantizando los atributos de la seguridad de la información (confidencialidad, disponibilidad e integridad).
4) **EL ENCARGADO** se obligará a respetar la propiedad de las Bases de Datos, por ende, no podrá hacer ninguna copia adicional de estas, salvo la de seguridad o aquella que sea necesaria para el cumplimiento de la finalidad del tratamiento, o sea exigido por la ley colombiana.
5) **EL ENCARGADO** deberá cumplir en todo caso con las obligaciones que la Ley Aplicable en materia de Datos Personales le confiere en su calidad de **ENCARGADO** del Tratamiento, eximiendo de cualquier responsabilidad al **RESPONSABLE** en caso de realizar un tratamiento por fuera del estipulado en el objeto de este Acuerdo.
6) **EL RESPONSABLE** garantiza a **EL ENCARGADO** que todos los datos personales que hagan parte de las bases de datos transmitidas han sido obtenidos de forma lícita y conforme a la legislación vigente, especialmente la Ley 1581 de 2012 y sus Decretos reglamentarios o las normas que las modifiquen o adicionen.
7) En caso de que de manera excepcional **EL ENCARGADO** realice transmisiones de datos, éstas deberán ser avaladas por **EL RESPONSABLE** y deberán soportarse en el respectivo documento de transmisión de datos personales.
8) Cada Parte responderá y eximirá de responsabilidad a la otra Parte, en caso de que alguna de sus actuaciones contraríe este Acuerdo, o alguna de ellas, haga un Tratamiento de los Datos Personales

incumpliendo la Ley Aplicable en materia de Datos Personales. Por lo anterior, **EL ENCARGADO** entiende que los Datos Personales transmitidos por **EL RESPONSABLE** podrán ser tratados únicamente para las finalidades indicadas en el objeto y alcance de este Acuerdo.

SEXTA – PROPIEDAD DE LA BASE DE DATOS: **EL ENCARGADO** reconoce y acepta que las Bases de Datos objeto de Transmisión, son de propiedad y administración exclusiva del METRO DE MEDELLÍN LTDA como **RESPONSABLE** de la información y que no se transferirá la propiedad de éstas.

SÉPTIMA – DURACIÓN: La transmisión de datos se realizará mientras subsista la relación enmarcada en el Contrato relacionado.

OCTAVA - USO DE HERRAMIENTAS CON INTELIGENCIA ARTIFICIAL, AUTOMATIZACIÓN AVANZADA Y TRANSFERENCIA DE TECNOLOGÍA

EL ENCARGADO reconoce que, en desarrollo del objeto contractual, podrá utilizar herramientas tecnológicas con capacidades de inteligencia artificial, automatización avanzada, análisis de código, pruebas automatizadas, monitoreo, diagnóstico, conversión técnica, trazabilidad o funcionalidades similares, exclusivamente para ejecutar la conversión, migración, configuración, integración, pruebas, estabilización, soporte y documentación de la plataforma ERP SAP ECC 6.0 EHP8 a SAP S/4HANA bajo modalidad RISE en AWS, conforme a las instrucciones documentadas de LA EMPRESA.

El uso de dichas herramientas no constituirá una autorización para tratar datos personales para finalidades propias de **EL ENCARGADO**, del fabricante de la herramienta, de sus proveedores, aliados, subcontratistas o terceros. En consecuencia, **EL ENCARGADO** no podrá utilizar datos personales, logs, incidencias, pantallas, reportes, código, configuraciones, metadatos, documentación, bases de datos, información transaccional o cualquier información de **EL RESPONSABLE** para entrenamiento, reentrenamiento, ajuste, mejora, validación, enriquecimiento, analítica propia, benchmarking, perfilamiento, scoring, monetización, reutilización en otros proyectos, desarrollo de productos, mejora de servicios propios o de terceros, ni para cualquier finalidad distinta a la ejecución del contrato.

Antes de utilizar cualquier herramienta con capacidades de inteligencia artificial, automatización avanzada, pruebas automatizadas, análisis de código, monitoreo o funcionalidades similares, **EL ENCARGADO** deberá informar y acreditar documentalmente a **EL RESPONSABLE**, como mínimo, lo siguiente:

a. Nombre de la herramienta, fabricante, versión, modalidad de licenciamiento y certificación o validación aplicable, incluyendo su inclusión en SAP Store / Marketplace cuando corresponda.

b. Funcionalidades específicas que serán utilizadas dentro del proyecto y actividades concretas en las que intervendrá la herramienta.

c. Tipo de información que será accedida, consultada, procesada, analizada, almacenada, transmitida o generada por la herramienta, diferenciando entre código, configuraciones, metadatos, logs, datos maestros, datos transaccionales, datos de prueba y datos personales reales.

d. Ambientes sobre los cuales operará la herramienta, distinguiendo entre DEV, QAS, PRD u otros ambientes autorizados por LA EMPRESA.

e. Indicación expresa de si la herramienta accede, trata, almacena, conserva o transfiere datos personales reales, así como la justificación de necesidad, proporcionalidad y minimización aplicable.

f. País o región donde se realizará el tratamiento, almacenamiento, soporte, monitoreo o acceso técnico a la información.

g. Identificación de proveedores, fabricantes, subcontratistas, subencargados, aliados tecnológicos o terceros que puedan tener acceso a información de LA EMPRESA a través de la herramienta.

h. Condiciones de conservación, eliminación, devolución, anonimización o supresión de la información tratada por la herramienta.

i. Medidas técnicas, administrativas, físicas, jurídicas y organizacionales aplicables, incluyendo control de accesos, cifrado, trazabilidad, segregación de ambientes, autenticación, registro de operaciones, gestión de incidentes y restricciones de descarga o extracción.

j. Declaración expresa de que la herramienta, su fabricante, **EL ENCARGADO**, sus proveedores, subencargados o terceros no utilizarán información de **EL RESPONSABLE** ni datos personales tratados por cuenta de esta para finalidades propias, entrenamiento, reentrenamiento, mejora de modelos, analítica, benchmarking, monetización o reutilización.

k. Términos de uso, condiciones de privacidad, documentación técnica, certificaciones, políticas de seguridad, acuerdos de procesamiento de datos, acuerdos de subencargo o documentos equivalentes aplicables a la herramienta.

El uso de datos personales reales en herramientas con inteligencia artificial, automatización avanzada, pruebas automatizadas, monitoreo, diagnóstico o análisis técnico será excepcional y requerirá autorización previa, expresa y documentada de **EL RESPONSABLE**. Como regla general, **EL ENCARGADO** deberá utilizar datos anonimizados, enmascarados, ficticios, ofuscados o minimizados en ambientes de desarrollo, calidad, pruebas, capacitación, demostración, automatización o validación, salvo que **EL RESPONSABLE** autorice expresamente el uso de datos reales por necesidad técnica debidamente justificada.

EL ENCARGADO no podrá incorporar datos personales reales, bases de datos, logs, pantallas, incidencias, evidencias, reportes o documentación de **EL RESPONSABLE** en herramientas externas, repositorios, ambientes, nubes, plataformas, servicios de inteligencia artificial, asistentes automatizados, motores de análisis, sistemas de pruebas o soluciones tecnológicas no autorizadas previamente por **EL RESPONSABLE**.

Previo al uso de estas herramientas, **EL RESPONSABLE** podrá realizar una evaluación preliminar documentada sobre el tratamiento de datos personales, transferencia de tecnología, privacidad desde el diseño y por defecto, seguridad, finalidad, necesidad, proporcionalidad, circulación restringida y responsabilidad demostrada. **EL ENCARGADO** deberá suministrar oportunamente toda la información requerida para dicha evaluación.

Cuando **EL RESPONSABLE** determine que el uso de la herramienta puede implicar tratamiento de datos personales reales de forma masiva, sistemática o no incidental; acceso a ambientes productivos; tratamiento

de datos sensibles o privados; decisiones automatizadas; perfilamiento; inferencias sobre titulares; transferencias internacionales no previstas; uso de información para entrenamiento o mejora de modelos; conservación por terceros; o cualquier otro escenario que pueda generar alto riesgo para los derechos de los Titulares, EL ENCARGADO no podrá iniciar dicho tratamiento hasta que EL RESPONSABLE realice la evaluación de impacto, análisis de riesgos o validación jurídica, técnica y organizacional que corresponda, y autorice expresamente su ejecución.

EL ENCARGADO deberá garantizar que las herramientas utilizadas no generen decisiones automatizadas con efectos jurídicos o significativos sobre empleados, proveedores, contratistas, usuarios, terceros o cualquier Titular de datos personales de EL RESPONSABLE. Cualquier funcionalidad de analítica, clasificación, recomendación, monitoreo, inferencia, predicción, scoring o perfilamiento que pueda afectar directa o indirectamente a personas naturales deberá ser informada previamente y no podrá ser utilizada sin autorización expresa y documentada de EL RESPONSABLE.

EL ENCARGADO será responsable por los actos, omisiones, accesos, tratamientos, conservaciones, transferencias, usos no autorizados, incidentes, vulneraciones de seguridad o incumplimientos derivados del uso de herramientas con inteligencia artificial, automatización avanzada, pruebas automatizadas, monitoreo, análisis técnico o funcionalidades similares, incluyendo aquellos imputables a sus empleados, proveedores, fabricantes, subencargados, aliados tecnológicos o terceros autorizados.

El incumplimiento de lo previsto en esta cláusula facultará a EL RESPONSABLE para suspender el uso de la herramienta, restringir accesos, ordenar la eliminación o devolución de la información, exigir evidencias de cumplimiento, solicitar medidas correctivas, suspender actividades del contrato relacionadas con tratamiento de datos personales y adoptar las acciones contractuales, administrativas o legales que resulten procedentes.

NOVENA – OBLIGACIONES DEL ENCARGADO: Además de los deberes establecidos en el artículo 18 de la Ley 1581 de 2012, serán obligaciones de EL ENCARGADO durante la ejecución del presente Acuerdo, las siguientes:

1. Dar aplicación a las obligaciones de EL RESPONSABLE bajo la Política de Tratamiento de Información y Datos Personales, la cual podrá encontrar en el siguiente link de su página web: https://www.metrodemedellin.gov.co/politicas-y-legales/proteccion-de-datos-personales/.
2. Dar tratamiento, a nombre de EL RESPONSABLE, a los Datos Personales conforme a los principios que los tutelan.
3. Realizar el Tratamiento de acuerdo con las finalidades establecidas en el objeto de este acuerdo, las autorizadas por los Titulares y con base en las Leyes aplicables, quedando expresamente prohibido exceder las mismas, como lo sería el uso de los datos para efectos propios del ENCARGADO.
4. Abstenerse de continuar tratando los Datos Personales objeto de Transmisión por EL RESPONSABLE, o de comunicarlos a terceros una vez las finalidades hayan cesado o la vigencia del Acuerdo haya terminado, a menos que el ENCARGADO recolecte autorización de tratamiento de datos a su nombre.

5. Adoptar las medidas de índole técnica, administrativa, organizativa y físicas necesarias, en materia de seguridad de la información, de acuerdo a la criticidad de la información personal a la que tenga acceso, en especial cuando la misma corresponda a datos sensibles y de menores de edad, para salvaguardar y garantizar la seguridad de los Datos Personales y evitar su alteración, pérdida, fuga, sustracción, Tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.
6. Declarar y garantizar que tratará los Datos teniendo en cuenta los niveles más altos de protección y confidencialidad y en cumplimiento de la Política de Tratamiento de la Información y Datos Personales de EL RESPONSABLE, la Ley Aplicable en materia de Protección de Datos Personales y cualquier instrucción adicional que EL RESPONSABLE le haya dado.
7. Dar estricto seguimiento a los elementos de la seguridad de la información, como lo son la confidencialidad, integridad y disponibilidad de los datos transmitidos.
8. Contar con una política de tratamiento de datos personales, un manual de políticas y procedimientos para el tratamiento de datos, un procedimiento para la atención y respuesta a consultas, peticiones y reclamos de los Titulares y toda la documentación que implica un Programa Integral de Gestión de Datos Personales.
9. Adoptar políticas o directrices donde se les informe a sus empleados sobre el uso de los Datos Personales que tratarán por cuenta de **EL RESPONSABLE,** de acuerdo con el objeto y alcance del Tratamiento definidos en las cláusulas segunda y tercera de este Acuerdo.
10. Atender de forma oportuna, apropiada y pertinente las solicitudes que le haga **EL RESPONSABLE** en relación con el Tratamiento de los Datos Personales sujetos a la Transmisión y cumplir con las recomendaciones emitidas por éste, así como con las sugerencias, instrucciones y ordenes de la Autoridad de Protección de Datos en Cumplimiento con la Ley Aplicable de Protección de Datos, en relación al Tratamiento de Datos Personales.
11. Colaborar con **EL RESPONSABLE** en todo lo relativo al cumplimiento de la legislación nacional.
12. En caso de presentarse un incidente de seguridad, entendiéndose por tal como la violación de los códigos de seguridad, o la pérdida, robo y acceso no autorizado, una fuga o una extracción sin previa autorización, **EL ENCARGADO** tendrá el deber de informar a **EL RESPONSABLE**, inmediatamente o a más tardar al día siguiente de su ocurrencia, para que este tome las medidas necesarias en el caso específico, debiendo dar gestión al incidente conforme a las normas y procedimientos establecidos; y en caso de ser necesario, prestar apoyo necesario para la notificación de los Titulares de los datos.

    Además de esto, deberá comunicar las brechas de seguridad que se hayan presentadas y las medidas tomadas.

    Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
b. El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
c. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
d. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

13. Permitir a **EL RESPONSABLE** auditar el cumplimiento de las obligaciones de protección de datos personales establecidas en este Acuerdo, tanto de **EL ENCARGADO**, como de sus subcontratistas que adquieran la calidad de **SUBENCARGADOS**.
14. Abstenerse de reproducir por cualquier medio los Datos Personales a los que tenga acceso en desarrollo de su encargo, salvo cuando ello resulte directa y absolutamente necesario para cumplir con las finalidades de este Acuerdo y siempre que medie autorización escrita otorgada por **EL RESPONSABLE**, evento en el cual las copias deben limitarse únicamente a la cantidad y la información autorizada.
15. Eliminar de sus servidores y sistemas de información de manera inmediata, la Base de Datos suministrada por **EL RESPONSABLE,** una vez se cumpla con las finalidades del Acuerdo e informarlo por medio escrito certificado dentro de los treinta (30) días calendario siguientes; a menos que **EL ENCARGADO** haya recolectado una autorización de tratamiento de datos personales a su nombre o exista un deber legal o contractual que lo obligue a archivar o almacenar la información tratada como evidencia de las actividades y gestión realizada, evento en el cual deberá implementar las medidas de seguridad necesarias, como lo podrá ser la anonimización, para garantizar la protección de la información personal .
16. No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios de **EL ENCARGADO**.

    Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al **RESPONSABLE**, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

    El subcontratista, que también tendrá la condición de **ENCARGADO** del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del

tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el **ENCARGADO** inicial seguirá siendo plenamente responsable ante **EL RESPONSABLE** en lo referente al cumplimiento de las obligaciones.

Así mismo **EL ENCARGADO** deberá celebrar un acuerdo o contrato donde se deje claro el alcance de los servicios que contratará con el subencargado y la manera en que se regulará esa transmisión.

17. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
18. Asistir al **RESPONSABLE** del tratamiento en la respuesta a las peticiones que interpongan los Titulares, en virtud del ejercicio de sus derechos.

NOVENA- OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO: Además de los deberes establecidos en el artículo 17 de la Ley 1581 de 2012, serán deberes de **EL RESPONSABLE** durante la ejecución del presente Acuerdo, los siguientes:

1. **EL RESPONSABLE** declara y garantiza que dará Tratamiento a los Datos Personales aplicando los más altos estándares de confidencialidad, en cumplimiento de su Política de Tratamiento de Información y Datos Personales y este Acuerdo.
2. **EL RESPONSABLE** notificará oportunamente a **EL ENCARGADO** acerca de cualquier cambio en la legislación que considere que puede afectar el Tratamiento de los Datos Personales o este Acuerdo.
3. **EL RESPONSABLE** resolverá de manera oportuna y adecuada todas las solicitudes realizadas por **EL ENCARGADO** en relación con el Tratamiento de los Datos Personales sujetos a la Transmisión.
4. Informar a **EL ENCARGADO** la política de tratamiento de datos implementada, a efectos de que éste pueda garantizar su cumplimiento íntegro y adecuado.
5. Informar a **EL ENCARGADO**, cuando sea procedente, sobre las reclamaciones y solicitudes de eliminación que realicen los Titulares de los Datos Personales, o las autoridades competentes, con el fin de suspender su Tratamiento, mientras la controversia es resuelta.
6. Contar con una política de tratamiento de datos personales, un manual de políticas y procedimientos para el tratamiento de datos, un procedimiento para la atención y respuesta a consultas, peticiones y reclamos de los Titulares y toda la documentación que implica un Programa Integral de Gestión de Datos Personales.
7. Garantizar que los Datos Personales que se le suministre a **EL ENCARGADO** sean conforme a la información suministrada por los Titulares.

DÉCIMA – MEDIDAS DE SEGURIDAD: EL ENCARGADO deberá tomar las medidas apropiadas desde el punto de vista administrativo, técnico, personal y físico para salvaguardar la información y los datos personales a los que tenga acceso, contra pérdida, robo, fuga, manipulación indebida, acceso no autorizado, modificación, divulgación y/o destrucción. Dentro de las mismas se encontrarán, pero no se limitarán a:

1. Políticas de Seguridad y privacidad de la Información: EL ENCARGADO debe contar con políticas de seguridad y privacidad de la información implementadas al interior de su empresa debidamente publicadas y aprobadas por la alta dirección y sus empleados deben contar con el conocimiento y apropiación de estas.
2. Gestión de riesgos de seguridad de la información y tratamiento de datos personales: EL ENCARGADO debe demostrar que tiene identificados y realiza una adecuada evaluación, tratamiento, control y seguimiento de los siguientes riesgos asociados a la protección de la integridad, disponibilidad y confidencialidad de los datos personales que serán tratados en virtud del servicio contratado.
    - Adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento a bases de datos personales.
    - Acceso no autorizado a sistema de información o redes de datos
    - Fuga de Información
    - Instalación y uso de software ilegal
    - Instalación de software malicioso
    - Fraude utilizando medios informáticos
    - Mala utilización de los equipos informáticos y redes de datos
    - Tratamiento inadecuado de datos personales
3. Protección de información confidencial o sensible: La información y datos sensibles y/o confidenciales a los que tenga acceso EL ENCARGADO a través de medios de almacenamiento externo o que se encuentre almacenada en sus equipos, bases de datos o sistemas de información, debe contar con las medidas de protección necesarias para prevenir el acceso, manipulación y modificación, extracción o transmisión no autorizados.
4. Comunicación segura: EL ENCARGADO debe contar con mecanismos de comunicación seguros, para garantizar que los datos personales e información sensible o confidencial que por cualquier motivo deba ser intercambiada con EL RESPONSABLE o terceros autorizados por esta, no sea vista, adulterada, modificada, transmitida o transferida a personas o entidades no autorizadas.
5. Acuerdos de confidencialidad: EL ENCARGADO debe realizar acuerdos de confidencialidad con los empleados, dependientes, contratistas o subcontratistas que tengan acceso a los datos personales, información sensible o confidencial.
6. Control de acceso a la información y cuartos de procesamiento de datos: EL ENCARGADO debe contar con medidas administrativas y técnicas para controlar el acceso físico y lógico a las bases de datos personales de EL RESPONSABLE, y en general, a la información según su clasificación, a los sistemas de información, centros de procesamiento de datos y equipos informáticos clasificados

como críticos. **EL ENCARGADO** debe garantizar que únicamente los usuarios autorizados, con el rol necesario y con acuerdo de confidencialidad vigente accedan a las bases de datos personales.

7. **Monitoreo de sistemas de información: EL ENCARGADO** debe demostrar que realiza el monitoreo permanente de las bases de datos, sistemas de información y la infraestructura tecnológica que los soporta, así como las actividades que realizan los usuarios autorizados y no autorizados con el fin de evitar afectaciones a la integridad, confidencialidad y disponibilidad de la información y actuar oportunamente en caso de cualquier evento o incidente de seguridad.
8. **Respaldo y recuperación de la información: EL ENCARGADO** debe demostrar que cuenta con mecanismos y rutinas periódicas para el respaldo de la información y su recuperación en caso de incidentes o desastres.
9. **Seguridad de los equipos de cómputo: EL ENCARGADO** custodiará la información entregada por **EL RESPONSABLE,** garantizando que esta será procesada o almacenada en equipos de cómputo y servidores autorizados, que cuenten con sistema operativo legal y actualizado a sus últimas versiones estables y con soporte técnico del fabricante y que tengan instalado software antivirus de uso corporativo, completamente actualizado y con soporte del fabricante.
10. **Seguridad de la red:** Los dispositivos a través de los cuales se haga tratamiento de los datos personales a los que tenga acceso **EL ENCARGADO** deberán estar protegidos por equipos de seguridad informática debidamente configurados que controlen el acceso y comunicaciones desde y hacia internet y que permitan mitigar el riesgo de ataque cibernético y fuga de información.
11. **Gestión de incidentes de seguridad informática: EL ENCARGADO** deberá contar con procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes de seguridad informática y datos personales. En dicho procedimiento deberán estar claramente establecidos los tiempos que aplica para la investigación de los incidentes y su reporte a las partes interesadas.

    EL ENCARGADO debe reportar a **EL RESPONSABLE** los eventos o incidentes de seguridad que afecten o tengan el potencial de afectar las bases de datos o datos a su cargo, la prestación del servicio contratado, la información intercambiada entre las partes, los sistemas de información de **EL RESPONSABLE** o la información alojada en estos, y todas aquellas situaciones de alto riesgo que sean detectadas por sus sistemas de monitoreo y control o las auditorías que realiza.
12. **Formación del personal**: **EL ENCARGADO** debe demostrar que ha instruido y capacitado a su personal en el adecuado manejo y reserva de la información y bases de datos personales a las que tiene acceso, así mismo, en el cumplimiento de las políticas de seguridad de la información y la detección y respuesta ante eventos e incidentes.
13. **Auditoría sobre los sistemas de información y bases de datos personales**: **EL ENCARGADO** debe demostrar que cuenta con una política de auditorías de seguridad de la información y bases de datos personales con el fin de identificar posibles vulnerabilidades que pongan en riesgo la información de **EL RESPONSABLE** y la disponibilidad de los servicios. Los protocolos de auditoría establecidos deben incluir la identificación y remediación de vulnerabilidades técnicas y administrativas sobre las

bases de datos personales, así como los sistemas de información, los equipos, la infraestructura tecnológica y las personas que intervienen en el tratamiento de los datos.

EL ENCARGADO deberá contar con la capacidad de demostrar que cumple con cada una de las medidas relacionadas.

EL RESPONSABLE durante la vigencia del contrato podrá realizar inspecciones y auditorías previamente acordadas con **EL ENCARGADO** para verificar el cumplimiento de los requisitos establecidos. El resultado de las auditorias que realice **EL RESPONSABLE** será compartido con **EL ENCARGADO** para que este realice la remediación de las vulnerabilidades encontradas en un plazo acordado entre las partes.

DÉCIMA PRIMERA - REQUERIMIENTOS: LAS PARTES convienen que cuando quiera que un Titular de los datos personales transmitidos o tratados por **EL ENCARGADO**, eleve una solicitud, queja o reclamo por el tratamiento que se le está dando a sus datos personales; relacionado con el objeto de este Acuerdo de transmisión; o una autoridad nacional, extranjera, administrativa o judicial presente un requerimiento que implique la revelación o divulgación de parte o la totalidad de la Información y/o Datos que han sido transmitidos, **EL ENCARGADO** informará por escrito a **EL RESPONSABLE,** a través del Supervisor del contrato, de dicha situación, en un plazo máximo de dos (2) días hábiles a partir de la recepción del mismo, y en todo caso, antes de hacer entrega de la Información, con el fin de que las Partes puedan tomar las medidas precisas para proteger sus intereses.

DÉCIMA SEGUNDA - DEVOLUCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN. Los Datos Personales tratados por **EL ENCARGADO** bajo el presente Acuerdo, continuarán bajo la custodia y control de **EL RESPONSABLE**; en ese sentido, cuando se cumpla el término de duración consagrado en la cláusula séptima del presente Acuerdo o alguna de las causales de terminación estipuladas en la cláusula décimo quinta, **EL ENCARGADO** deberá devolver y/o destruir la información de acuerdo con lo que decida **EL RESPONSABLE** de los datos Personales o, cuando sea aplicable, borrarla permanente e irrevocablemente de la o las computadoras y demás sistemas bajo control de **EL ENCARGADO** o de cualesquiera de sus empleados. A menos que éste cuente con la debida autorización de los Titulares de los datos, para que los mismos hagan parte de sus Bases de Datos o exista un deber legal o contractual de almacenar o archivar la información.

DÉCIMA TERCERA – RESPONSABILIDAD: EL ENCARGADO se compromete expresamente a eximir de cualquier responsabilidad civil, penal o administrativa a **EL RESPONSABLE** dejándolo indemne de cualquier indemnización o sanción, en caso de emplear los Datos Personales suministrados para usos no autorizados y se presenten requerimientos por parte del Titular o de entidades administrativas o judiciales, como consecuencia del mal proceder de **EL ENCARGADO,** causando daños y perjuicios.

En los casos de uso no autorizado o divulgación, **EL ENCARGADO**, deberá desplegar los esfuerzos necesarios para la recuperación de los Datos Personales y la prevención de su uso, divulgación o venta; facultando a **EL RESPONSABLE**, para solicitar que sea indemnizado por los daños y perjuicios que se le causen como consecuencia del incumplimiento de sus obligaciones bajo este Acuerdo.

Así mismo **EL RESPONSABLE** podrá repetir contra **EL ENCARGADO** por las sumas de dinero que en virtud de sanciones se le imponga por parte de las autoridades competentes, como consecuencia de algún incumplimiento legal o contractual atribuible a **EL ENCARGADO**.
Cualquier uso ilegal o contrario a las finalidades establecidas en el presente Acuerdo por parte de **EL ENCARGADO** conlleva la exención total de responsabilidad por parte de **EL RESPONSABLE.**

DÉCIMA CUARTA - CAUSALES DE TERMINACIÓN: El presente Acuerdo terminará por las siguientes causales: a) por el incumplimiento de las obligaciones adquiridas por alguna de las Partes; b) Por el Tratamiento de los Datos Personales por fuera de las finalidades señaladas en el presente Acuerdo; c) cuando se cumpla el término de duración descrito en la cláusula séptima del presente Acuerdo y; d) en los demás casos previstos en el presente Acuerdo.

DÉCIMA QUINTA - LEY Y DOMICILIO: Las normas que rigen el presente contrato son las inherentes a la materia contratada, en especial la Ley 1581 de 2012, el Decreto 1074 de 2015, y demás normas concordantes y se tiene como domicilio para todos los efectos legales el Municipio de Bello (Ant).

NOTA: El presente anexo es desarrollo de la cláusula denominada TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES del contrato No. 009104C-26 y hace parte integrante de la misma.