UNIDAD ADMINISTRATIVA ESPECIAL CUERPO OFICIAL DE BOMBEROS

PROCESO No. UAECOB-CMA-004-2026

ANEXO No. 6

CERTIFICACIÓN DE EXISTENCIA O NO DE SITUACIONES DE CONTROL

Bogotá, (día, mes, año)

Señores:
UAE CUERPO OFICIAL DE BOMBEROS BOGOTÁ
Ciudad.

Referencia: UAECOB-CMA-004-2026

Respetados señores:

Nosotros los suscritos _____ (nombre del proponente), identificado con (nit, cc, etc)_____, de conformidad con las condiciones que se estipulan en los documentos del Proceso de selección No. UAECOB-CMA-004-2026, y en atención a lo señalado en el Decreto 1600 de 2024 en su artículo 2.1.4.3.2.1 "Prevención de corrupción en la contratación pública", en el numeral a), manifestamos bajo la gravedad de juramento que:

1. Que la empresa a la que representa o alguno de los integrantes de la sociedad a la que represento participa **(SI) o (NO) (diligencie según aplique)** en una situación de control con otra persona natural, jurídica o proponente plural que se encuentra participando en el proceso de selección No. UAECOB-CMA-004-2026.

2. Que la empresa a la que representa o alguno de los integrantes de la sociedad a la que represento (**SI) o (NO) (diligencie según aplique)** se encuentra controlada por otra persona natural, jurídica o proponente plural que se encuentra participando en el proceso de selección No. UAECOB-CMA-004-2026.

3. Que la empresa a la que representa o alguno de los integrantes de la sociedad a la que **represento (SI) o (NO) (diligencie según aplique)** es controlante de otra persona natural, jurídica o proponente plural que se encuentra participando en el proceso de selección No. UAECOB-CMA-004-2026.

4. Que la empresa a la que representa o alguno de los integrantes de la sociedad a la que represento (**SI) o (NO) (diligencie según aplique)** comparte la condición de controlante con otra persona natural, jurídica o proponente plural que se encuentra participando en el proceso de selección No. UAECOB-CMA-004-2026.

Atentamente,

NOMBRE COMPLETO DEL PROPONENTE: _____

Nit: _____

Régimen tributario al cual pertenece: _____

Correo electrónico: _____

Dirección: _____

Nombre del representante legal: _____

FIRMA DEL PROPONENTE Y/O REPRESENTANTE LEGAL (*): _____

(*) NOTA: Esta certificación deberá ser presentada y firmada por el proponente con la propuesta respectiva. Si es persona jurídica, por quien conforme a la ley esté facultado; Si es consorcio o unión temporal por quien haya sido designado representante en el documento de constitución; Si actúa en calidad de apoderado, debe estar debidamente facultado por quien tenga la legitimación para hacerlo, caso en el cual debe anexar el poder correspondiente, con la debida presentación personal.

NOTA 2: El proponente plural debe diligenciar por cada uno de sus integrantes.

FORMATO No. 7
COMPROMISO ANTICORRUPCIÓN

Bogotá, D.C.

Señores
UAE - Cuerpo Oficial de Bomberos

Proceso de Contratación **UAECOB-CMA-004-2026**

[Nombre del representante legal o de la persona natural Proponente], identificado como aparece al pie de mi firma, [obrando en mi propio nombre o en mi calidad de representante legal de] [nombre del Proponente], manifiesto que:

1. Apoyamos la acción del Estado colombiano y de la UAE - Cuerpo Oficial de Bomberos para fortalecer la transparencia y la rendición de cuentas de la administración pública.

2. No estamos en causal de inhabilidad alguna para celebrar el contrato objeto del Proceso de Contratación [Insertar información].

3. Nos comprometemos a no ofrecer y no dar dádivas, sobornos o cualquier forma de halago, retribuciones o prebenda a servidores públicos o asesores de la Entidad Contratante, directamente o a través de sus empleados, contratistas o tercero.

4. Nos comprometemos a no efectuar acuerdos, o realizar actos o conductas que tengan por objeto o efecto la colusión en el Proceso de Contratación [Insertar información.

5. Nos comprometemos a revelar la información que sobre el Proceso de Contratación [Insertar información] nos soliciten los organismos de control de la República de Colombia.

6. Nos comprometemos a comunicar a nuestros empleados y asesores el contenido del presente Compromiso Anticorrupción, explicar su importancia y las consecuencias de su incumplimiento por nuestra parte, y la de nuestros empleados o asesores.

7. Conocemos las consecuencias derivadas del incumplimiento del presente compromiso anticorrupción.

En constancia de lo anterior firmo este documento a los [Insertar información] días del mes de [Insertar información] de [Insertar información].

_____
[Firma representante legal del Proponente o del Proponente persona natural]
Nombre: [Insertar información]
Cargo: [Insertar información]
Documento de Identidad: [Insertar información]

UNIDAD ADMINISTRATIVA ESPECIAL CUERPO OFICIAL DE BOMBEROS

PROCESO No. UAECOB-CMA-004-2026

ANEXO No. 08

AUTORIZACIÓN CONSULTA REGISTRO INHABILIDADES POR DELITOS SEXUALES COMETIDOS CONTRA MENORES DE EDAD

Bogotá DC, **Haga clic aquí o pulse para escribir una fecha.**

Yo **Escriba su nombre** identificado con cédula **Escriba el número de su documento de identidad** autorizo libre, expresa, inequívoca y exclusivamente, a la **Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá**, a consultar mis datos personales en el registro de inhabilidades por delitos sexuales cometidos contra menores edad que administra el Ministerio de Defensa - Policía Nacional de Colombia, en los términos señalados en la Ley 1918 de 2018 (*Por medio de la cual se establece el régimen de inhabilidades a quienes hayan sido condenados por delitos sexuales cometidos contra menores, se crea el registro de inhabilidades y se dictan otras disposiciones*), reglamentada por el Decreto 753 de 2019 (*Por medio del cual se reglamenta la Ley 1918 de 2018 (Por medio de la cual se establece el régimen de inhabilidades a quienes hayan sido condenados por delitos sexuales cometidos contra menores, se crea el registro de inhabilidades y se dictan otras disposiciones*), como requisito previo para mi eventual contratación y, de llegarse a formalizar ésta, cada cuatro (4) meses a partir del inicio de ésta, o cuando sea requerido, y mientras se encuentre vigente.

Así mismo, declaro que conozco que la recolección y tratamiento de mis datos se realizará de conformidad con la normatividad vigente sobre protección de datos personales, en especial la Ley 1581 de 2012, el Decreto 1074 de 2015 y la Política de Tratamiento de Datos Personales que podrá consultar en: https://www.bomberosbogota.gov.co/content/sc-po-01-politica-proteccion-y-tratamiento-datos-personales, manifestando que he sido informado(a) de forma clara y suficiente de los fines de su tratamiento.

_____

Firma

Nombre: **Haga clic para escribir texto**

Cédula No: **Haga clic para escribir número**

UNIDAD ADMINISTRATIVA ESPECIAL CUERPO OFICIAL DE BOMBEROS

PROCESO No. UAECOB-CMA-004-2026

Anexo No. 09

Con este acuerdo se dan a conocer las obligaciones que deberán aceptar los proveedores y contratistas (en adelante EL RECEPTOR), que conozcan o puedan conocer de corrupción, así como respecto al manejo, operación o administración de información privada, semi privada, información pública reservada, pública clasificada, en el desarrollo de sus funciones u obligaciones, trámite de peticiones ciudadanas, por presuntos hechos de corrupción, o en el manejo de sistemas de información o repositorios corporativos, considerando que en estos se centraliza la información de LA ENTIDAD y otras condiciones respecto a propiedad intelectual.

EN CONSECUENCIA, SE FIRMA EL SIGUIENTE:

ACUERDO DE CONFIDENCIALIDAD

Entre la **UNIDAD ADMINISTRATIVA ESPECIAL CUERPO OFICIAL DE BOMBEROS DE BOGOTÁ** o para efectos del presente documento **LA ENTIDAD**, con **NIT.899.999.061**, representada legalmente por **PAULA XIMENA ESCOBAR HENAO**, en su calidad de Representante Legal de la Entidad, y por la otra parte **[NOMBRE COMPLETO DEL CONTRATISTA/ PROVEEDOR],** identificado(a) con **[Tipo y Número de Identificación],** [en caso de ser persona jurídica, añadir: con NIT. **[Número de NIT],** representada legalmente por **[Nombre del Representante Legal]** identificado(a) **con [Tipo y Número de Identificación]]** o para efectos del presente documento EL RECEPTOR, hemos acordado celebrar el presente Acuerdo de Confidencialidad, Seguridad de la Información y Propiedad Intelectual el cual se regirá por las siguientes cláusulas teniendo en cuenta las:

CONSIDERACIONES

Que el marco regulatorio actual establece una serie de condiciones y obligaciones para el manejo responsable de la información, debido a que un mal uso de la misma podría conllevar la vulneración de derechos constitucionales como la intimidad, el habeas data y la información pública. En este sentido y teniendo en cuenta los casos específicos relativos a la actividad contractual, la entidad se rige por:

- **Ley 80 de 1993 (Estatuto General de Contratación de la Administración Pública)**: Esta ley establece las reglas y principios que rigen los contratos de las entidades estatales. Define el contrato de prestación de servicios como una figura para que las entidades realicen actividades de administración u operación que no puedan ser atendidas con el personal de planta. Su artículo 13 permite que los contratos estatales se rijan por las normas comerciales y civiles en aquellas materias no reguladas por el estatuto.
- **Ley 1150 de 2007**: Introduce medidas de eficiencia y transparencia. El literal h) del numeral 4 del artículo 2 establece que la selección del contratista para servicios profesionales y de apoyo a la gestión se realiza, por regla general, a través de la modalidad de contratación directa.
- **Normativa Complementaria y Guías Técnicas**:
- **Consejo de Estado**: Ha ratificado la posibilidad de que las entidades públicas celebren contratos de licencia o cesión, propios del derecho privado, para la explotación de sus activos intangibles.
- **Superintendencia Financiera de Colombia (SFC)**: Exige que los proveedores de servicios en la nube ofrezcan una disponibilidad de al menos el 99.95% para modelos de servicio como IaaS y PaaS, y del 99.5% para SaaS.
- **Procuraduría General de la Nación (PGN)**: Ha exigido en sus términos de referencia que las plataformas de nube contratadas cuenten con certificaciones internacionales como ISO 27018 para la protección de datos personales en la nube e ISO 22301 para la continuidad del negocio.
- **Colombia Compra Eficiente (CCE)**: Sus acuerdos marco de precios y guías de contratación, como la de propiedad intelectual, establecen lineamientos sobre borrado seguro de datos y la transferencia de derechos patrimoniales a la entidad.
- **Constitución Política de Colombia (Artículo 15)**: Consagra el derecho fundamental a la intimidad y el hábeas data, que permite a todas las personas conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos.
- **Ley Estatutaria 1581 de 2012 - Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022.**: Es la ley marco de protección de datos personales. Desarrolla el derecho constitucional al hábeas data y define los principios para el tratamiento de datos. Asigna a la Superintendencia de Industria y Comercio (SIC) la facultad de vigilancia y sanción.
- **Ley 1266 de 2008- Parcialmente Reglamentada por el Decreto 1081 de 2015.**: Regula el manejo de la información contenida en bases de datos personales de naturaleza financiera, crediticia, comercial y de servicios.
- **Ley 1712 de 2014 (Ley de Transparencia)**: Regula el derecho de acceso a la información pública bajo el principio de "máxima publicidad", que establece que toda información en posesión de una entidad pública es pública, salvo las excepciones constitucionales o legales.
- **Ley 594 de 2000 (Ley General de Archivo)**: Dicta las disposiciones sobre la gestión documental y la organización de los archivos públicos y privados.
- **Ley 527 de 1999- Desarrollado por el Decreto 4487 de 2009 - Reglamentado parcialmente por el Decreto 1747 de 2000.**: Define y reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales.
- **Decreto 1377 de 2013**: Reglamenta parcialmente la Ley 1581 de 2012, buscando garantizar la protección del derecho de hábeas data en aspectos como la autorización para el tratamiento de datos personales.
- **Resolución 1519 de 2020 (MinTIC)**: Define los estándares y directrices para publicar la información de la Ley 1712, incluyendo requisitos en materia de accesibilidad web, seguridad digital y datos abiertos.
- **Decreto 1078 de 2015 (DUR-TIC)**: Establece el marco para la Política de Gobierno Digital, en la cual la seguridad y privacidad de la información es un habilitador transversal.
- **Decreto 2106 de 2019**: Señala la obligatoriedad de disponer de una estrategia de seguridad digital para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos del MinTIC.
- **Resolución 500 de 2021 del MinTIC**: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

Esta resolución obliga a las entidades a adoptar medidas técnicas, administrativas y de talento humano para incorporar la seguridad digital en el plan de seguridad y privacidad de la información y mitigar riesgos.

- **Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC**: Define el Modelo de Seguridad y Privacidad de la Información (MSPI) basado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), integrando consideraciones y controles específicos de ciberseguridad.
- **Lineamientos de Roles y Responsabilidades del MinTIC**: Detalla las funciones y responsabilidades asociadas a la seguridad y privacidad de la información que deben ser asumidas por los servidores públicos, colaboradores y terceros.
- **Resolución 02277 DE 2025 (junio 3) de MinTIC** Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia. Dentro de estos se realiza énfasis en la nueva función de ciberseguridad denominada Gobernabilidad, estableciendo nuevos roles y responsabilidades especialmente a nivel Directivo.
- **Resolución 746 de 2022 "**Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.**"**
- **Manual de políticas de seguridad y privacidad de la información**. Establece las políticas específicas de seguridad y privacidad de la información que permitan reducir amenazas y vulnerabilidades de los activos de información de la Unidad Administrativa Especial Cuerpo Oficial Bomberos de Bogotá (UAECOB), enfocadas en afianzar los principios de confidencialidad, disponibilidad e integridad de la información, con el fin de asegurar la continuidad del negocio y gestionar los riesgos asociados interpretado conforme los términos de la norma ISO 22301 sobre las buenas prácticas.

Que la entidad, en el marco de la formulación e implementación de su Modelo de Seguridad y Privacidad de la Información (MSPI), requiere asegurar que todas las partes que accedan manejen, operen o administren información de la entidad, ya sea privada, semiprivada, pública reservada o pública clasificada, cumplan con los más altos estándares de protección de la información y ciberseguridad, así como con la protección de los derechos de autor que puedan recaer sobre la misma.

Que EL RECEPTOR, en virtud de la relación contractual o de colaboración con LA ENTIDAD, tendrá acceso a información clasificada y de carácter confidencial, y es necesario establecer las condiciones para su adecuado manejo y protección.

CLÁUSULAS

PRIMERA: DEFINICIONES.

Para los efectos del presente Acuerdo, los siguientes términos tendrán el significado que a continuación se indica:

- **Modelo de Seguridad y Privacidad de la Información (MSPI)**: Modelo definido por el Ministerio de Tecnologías de la Información y las Comunicaciones para formalizar al interior de las entidades un Sistema de Gestión de Seguridad y Privacidad de la Información y seguridad digital, el cual contempla su operación basada en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), integrando consideraciones y controles específicos de ciberseguridad en cada una de sus etapas.
- **Seguridad de la Información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital.
- **Confidencialidad**: Propiedad que garantiza que la información no está disponible ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: Propiedad que salvaguarda la exactitud y completitud de la información y los métodos de procesamiento.
- **Disponibilidad**: Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.

- **Ciberseguridad**: Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, a través de la protección de la información, de los servicios tecnológicos, los sistemas de información, la infraestructura tecnológica y las redes que, en conjunto, constituyen el entorno digital en el país.
- **Información Confidencial**: Cualquier información o material técnico o de negocio, incluyendo, pero sin limitarse a, datos, software, diseños, programas de computadora, secretos comerciales, informes, planes de negocio, estrategias, estudios, estadísticas, información financiera, información de clientes o proveedores, bases de datos, contraseñas, códigos fuente, datos personales y cualquier otro conocimiento o dato, sin importar su soporte (físico, electrónico, verbal, visual, etc.), que sea propiedad de LA ENTIDAD o a la que EL RECEPTOR tenga acceso en virtud de la relación con LA ENTIDAD, y que no sea de conocimiento público.
- **Información Clasificada**: (Remitirse a la definición establecida en la Ley 1712 de 2014 y el Documento Maestro del MSPI). Información que por su naturaleza podría causar daño si se divulga, modifica o destruye sin autorización.
- **Información Pública Reservada**: (Remitirse a la definición establecida en la Ley 1712 de 2014 y el Documento Maestro del MSPI). Información que, aun siendo pública, su acceso está restringido por ley por razones específicas.
- **Activos de Información**: Cualquier información o sistema de información que tenga valor para la entidad. Esto incluye datos, sistemas de información, software, equipos, servicios y personal.
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Gestión de Incidentes de Seguridad Digital:** Conjunto de actividades para identificar, reportar, analizar, contener, erradicar y recuperar ante incidentes que afecten la confidencialidad, integridad o disponibilidad de la información.
- **Trazabilidad de Accesos:** Registro verificable de quién accede, modifica, consulta o elimina información, incluyendo fecha, hora, repositorio y tipo de operación.

SEGUNDA: OBJETO.

El presente Acuerdo tiene por objeto establecer las condiciones bajo las cuales EL RECEPTOR deberá cumplir, manejar y proteger y garantizar la Información Confidencial, Información Clasificada, Información Pública Reservada, datos personales y cualquier otro tipo de información que LA ENTIDAD le revele o a la que EL RECEPTOR tenga acceso en desarrollo de la relación contractual o de colaboración, garantizando su confidencialidad, integridad, disponibilidad y los derechos de autor.

TERCERA: DE LA CONFIDENCIALIDAD, RESERVA Y NO DIVULGACIÓN DE LA INFORMACIÓN.

EL RECEPTOR reconoce y acepta que, en virtud del presente Contrato/Convenio, tendrá acceso a Información Confidencial, Información Clasificada, Información Pública Reservada, datos personales y cualquier otro tipo de información, en formato físico o digital, que sea propiedad o esté bajo custodia de LA ENTIDAD.

Definición de Información Confidencial: Para los efectos de la presente cláusula, se entenderá como "Información Confidencial" cualquier información técnica, financiera, operativa, administrativa, legal, de seguridad, estratégica o de cualquier otra naturaleza que la ENTIDAD revele al RECEPTOR o que este último llegue a conocer, generar o desarrollar en el marco de la relación con la entidad, ya sea que esté contenida en documentos escritos, digitales, verbales o cualquier otro medio. Esto incluye, sin limitarse a, datos personales, códigos fuente, bases de datos, protocolos de seguridad, algoritmos, y cualquier activo intangible que sea desarrollado por el RECEPTOR, el cual reconoce que la información confidencial puede incluir información pública que, por su naturaleza o por requerimientos de seguridad, necesita un tratamiento especial y no divulgación masiva.

EL RECEPTOR se obliga a:

1. **Preservar la Confidencialidad:** Mantener en estricta reserva y confidencialidad toda la Información Confidencial, Clasificada, Pública Reservada y datos personales a la que acceda, utilice, procese, transmita o almacene, durante la ejecución del presente Contrato/Convenio y de manera indefinida una vez finalizada la relación contractual, a menos que su divulgación sea expresamente autorizada por escrito por LA ENTIDAD o requerida por ley o autoridad competente.
2. **Uso Exclusivo**: Utilizar la información únicamente para los fines específicos y autorizados del presente Contrato/Convenio, prohibiéndose cualquier uso no autorizado, incluyendo su reproducción, copia, modificación, difusión o comercialización.
3. **No Divulgación**: Abstenerse de divulgar, revelar, publicar, transferir o facilitar, por cualquier medio, la Información Confidencial, Clasificada, Pública Reservada y datos personales a terceros no autorizados, incluyendo personal propio que no requiera conocer dicha información para el cumplimiento de sus funciones.
4. **Clasificación de la Información**: Reconocer y respetar el esquema de clasificación de la información adoptado por LA ENTIDAD, de acuerdo con los "Lineamientos del Modelo de Seguridad y Privacidad de la Información" del MinTIC, y aplicar las medidas de protección correspondientes a cada nivel de clasificación.
5. **Protección de Datos Personales**: Cumplir estrictamente con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios en materia de protección de datos personales. Esto incluye, pero no se limita a, la recolección, almacenamiento, uso, circulación o supresión de datos personales bajo los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Deberá adoptar las medidas de seguridad necesarias para proteger la información personal, incluyendo cifrado, control de acceso y monitoreo, en alineación con las legislaciones de privacidad pertinentes.
6. **Medidas de Seguridad**: Implementar y mantener medidas de seguridad técnicas, administrativas y físicas adecuadas para proteger la información de accesos no autorizados, alteración, divulgación o destrucción, de conformidad con los "Lineamientos del Modelo de Seguridad y Privacidad de la Información" y la "Resolución 500 de 2021" del MinTIC. Esto incluye la aplicación de controles para mitigar los riesgos identificados en el análisis de riesgos de LA ENTIDAD. Dentro de las medidas de seguridad técnicas el receptor se obliga a mantener o almacenar la información corporativa únicamente en los repositorios corporativos brindados por la dependencia de Tecnología de la Entidad.
7. **Notificación de Incidentes**: Notificar de manera inmediata a LA ENTIDAD sobre cualquier incidente de seguridad de la información o de datos personales, sospecha de acceso no autorizado, divulgación indebida, pérdida, alteración o destrucción de la información, de acuerdo con el procedimiento de gestión de incidentes de seguridad digital establecido por LA ENTIDAD y los lineamientos del MinTIC.
8. **Retorno o Destrucción de la Información**: A la terminación o finalización del presente Contrato/Convenio, por cualquier causa, EL RECEPTOR se compromete a devolver a LA ENTIDAD toda la Información Confidencial, Clasificada, Pública Reservada y datos personales, incluyendo copias, o a destruirla de forma segura, según las instrucciones de LA ENTIDAD, y a certificar por escrito su cumplimiento. Se deberán verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar la eliminación segura o reutilización.
9. **Responsabilidades del Personal**: EL RECEPTOR será responsable de asegurar que su personal, subcontratistas o cualquier tercero bajo su control que tenga acceso a la información, cumpla con las mismas obligaciones de confidencialidad y no divulgaciones aquí establecidas.
10. **Acuerdos Individuales de Confidencialidad:** EL RECEPTOR deberá garantizar que todo su personal, subcontratistas o terceros que accedan a información de LA ENTIDAD firmen acuerdos individuales de confidencialidad, los cuales deberán ser entregados a LA ENTIDAD antes del inicio de actividades.

PARÁGRAFO 1: **ALMACENAMIENTO, RESPALDO Y BORRADO SEGURO**

El ciclo de vida completo de los datos, desde su creación hasta su eliminación, será detallado en la información documentada de los procesos de acuerdo con el mapa de procesos y el Modelo Integral de Planeación y Gestión que definirá todos los aspectos para la gestión en la nube, la cual puede garantizarse a nivel lógico de acuerdo con los flujos de los procesos.

Desde la dependencia de Dirección -TICS de la Entidad se establecerá los mecanismos que permitan contar con un respaldo de la información procesada, el cual deberá estar a disposición de la entidad en cualquier momento. Al finalizar el contrato, el borrado seguro de los datos existentes en los medios de almacenamiento es una obligación fundamental. En caso de contratarse servicios de nube el proveedor de nube se compromete a brindar un acompañamiento apropiado ante una terminación de contrato para el traslado de los servicios tecnológicos a otro proveedor, de igual manera a brindar el tiempo suficiente para el retiro de los servicios tecnológicos. Así como reportar oportunamente los incidentes y/o cambios que se tengan en la plataforma tecnológica que soporta los servicios de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos. De igual manera es importante que el proveedor de nube brinde un plan de continuidad de negocio que contemple el servicio o servicios tercerizados por la UAE Cuerpo Oficial de Bomberos Bogotá.

CUARTA: DE LOS DERECHOS DE AUTOR Y PROPIEDAD INTELECTUAL.

PARÁGRAFO 1: Titularidad de la Obra por Encargo: EL RECEPTOR declara y garantiza que todos los desarrollos de software, códigos fuente, bases de datos, diseños, metodologías, informes, manuales y cualquier otra obra o activo intangible (en adelante, "las Obras") que sean creados, desarrollados o entregados en desarrollo de su relación con la ENTIDAD, son de su exclusiva autoría. De conformidad con el artículo 13 de la Ley 80 de 1993 y el régimen de propiedad intelectual aplicable, las partes acuerdan expresamente que los derechos patrimoniales sobre las Obras pertenecerán a la ENTIDAD.

PARÁGRAFO 2: Alcance de la Cesión: La cesión de derechos patrimoniales a favor de la ENTIDAD incluye, entre otros, los derechos de reproducción, distribución, transformación, comunicación pública, puesta a disposición de forma ilimitada y cualquier otro derecho conocido o por conocerse, en todas las modalidades de explotación y formas de utilización que sean posibles en el ambiente análogo, digital o cualquier otro entorno tecnológico. Las partes acuerdan que esta transferencia de derechos patrimoniales es definitiva, irrevocable y tendrá la misma duración que establece la ley autoral vigente en Colombia, sin limitación alguna en cuanto a territorio se refiere.

PARÁGRAFO 3: Derechos Morales: Las partes reconocen y aceptan que la cesión aquí pactada se limita a los derechos patrimoniales y que los derechos morales de autor sobre las Obras permanecerán en cabeza de su creador, conforme a lo establecido en la Ley 23 de 1982. El RECEPTOR, sin embargo, autoriza a la ENTIDAD a divulgar las Obras, siempre que se respete la autoría.

PARÁGRAFO 4: Indemnidad: El RECEPTOR garantiza la originalidad de las Obras y que no vulneran los derechos de propiedad intelectual de terceros. En consecuencia, se obliga a asumir la defensa legal y a indemnizar a la ENTIDAD por cualquier reclamación, litigio o gasto que pueda surgir por la supuesta violación de derechos de autor, patentes, marcas o cualquier otra figura de propiedad intelectual, liberando a la ENTIDAD de toda responsabilidad.

Además, y respecto a estos aspectos de la propiedad intelectual se tendrá en cuenta lo siguiente:

1. **Titularidad**: EL RECEPTOR reconoce que toda obra, desarrollo de software, bases de datos, documentos, informes, metodologías, contenidos materiales, desarrollos, mejoras, los derechos de autor, propiedad intelectual, patentes, marcas, diseños, modelos de utilidad, secretos industriales y cualquier otro derecho de propiedad intelectual o cualquier

otra creación o resultado derivado de la ejecución del Contrato/Convenio, serán de propiedad exclusiva de LA ENTIDAD, salvo que se pacte lo contrario de manera expresa y por escrito.

2. **Cesión de Derechos:** En caso de que EL RECEPTOR genere obras o desarrollos susceptibles de protección por derechos de autor o propiedad intelectual en el marco de este Contrato/Convenio, se entenderá que todos los derechos patrimoniales sobre dichas obras o desarrollos son cedidos a LA ENTIDAD de forma exclusiva, ilimitada y para todos los usos y medios, a partir de su creación, sin que EL RECEPTOR pueda reclamar compensación adicional a la pactada en este Contrato/Convenio.
3. **Uso Autorizado**: EL RECEPTOR podrá utilizar los materiales protegidos por derechos de autor de LA ENTIDAD únicamente en la medida necesaria para cumplir con las obligaciones del presente Contrato/Convenio y bajo las condiciones y restricciones que LA ENTIDAD establezca.
4. **No Infracción**: EL RECEPTOR declara que los servicios y productos que provea a LA ENTIDAD no infringirán derechos de autor o de propiedad intelectual de terceros, y mantendrá indemne a LA ENTIDAD frente a cualquier reclamo o demanda por infracción de estos derechos.

QUINTA: AUDITORIA DE CUMPLIMIENTO.

LA ENTIDAD se reserva el derecho de auditar en cualquier momento, con previo aviso a EL RECEPTOR, para verificar el cumplimiento de las obligaciones de confidencialidad, seguridad de la información y protección de datos personales establecidas en el presente Contrato/Convenio y en la normativa vigente. EL RECEPTOR deberá brindar todas las facilidades y colaboración necesarias para la realización de dicho seguimiento.

El receptor se compromete a utilizar únicamente los repositorios corporativos brindados por la oficinaTIC, para almacenar los archivos digitales generados durante la vigencia de este contrato.

SEXTA: CONSECUENCIAS DEL INCUMPLIMIENTO.

El incumplimiento por parte de EL RECEPTOR de cualquiera de las obligaciones de confidencialidad, seguridad de la información, protección de datos personales o derechos de autor estipuladas en el presente Contrato/Convenio, dará lugar a las acciones legales, contractuales y pecuniarias que LA ENTIDAD considere pertinentes, sin perjuicio de las responsabilidades penales y administrativas a que haya lugar conforme a la legislación colombiana.

SÉPTIMA: LEGISLACIÓN APLICABLE Y SOLUCIÓN DE CONTROVERSIAS.

El presente Acuerdo se regirá e interpretará de acuerdo con las leyes de la República de Colombia. Cualquier controversia o diferencia que surja entre las partes con ocasión de la interpretación, ejecución o cumplimiento del presente Acuerdo, se intentará resolver de manera amigable y directa. En caso de no ser posible, la controversia se someterá a la jurisdicción ordinaria de los jueces de la República de Colombia.

OCTAVA: VIGENCIA Y DEVOLUCIÓN: el contenido del presente acuerdo permanecerá vigente durante el plazo de existencia de la relación contractual entre LA ENTIDAD y EL RECEPTOR y por un término adicional de cinco (5) años contados a partir de su finalización, sin perjuicio de la aplicación de la Ley 1581 de 2012 y sus decretos reglamentarios para el manejo de datos

personales. Al finalizar la relación, EL RECEPTOR deberá devolver a la ENTIDAD toda la Información Confidencial en su poder y certificar su destrucción segura y definitiva de sus sistemas.

Para constancia, se firma el presente Acuerdo a los [Día] días del mes de [Mes] del año [Año],

LA ENTIDAD

EL RECEPTOR

[Nombre Completo del Contratista/Colaborador/Proveedor] [Tipo y Número de Identificación] [En caso de persona jurídica, añadir: Representante Legal]