Contraloría
Departamental del Valle del Cauca

120-11-01

COMPLEMENTO A LA
COMUNICACIÓN ACEPTACIÓN DE OFERTA DEL PROCESO DE SELECCIÓN DE MINIMA CUANTÍA No.006-2026

OBJETO: ***"Adquirir doscientas cincuenta (250) licencias del antivirus ESET PROTECT Complete, correspondientes a la renovación del licenciamiento para la protección, detección y eliminación de virus, troyanos, gusanos, adware, spyware, phishing, rootkits y archivos maliciosos."***

Santiago de Cali, ocho (08) de octubre de 2026

LINA MARCELA VÁSQUEZ VARGAS, mayor de edad, domiciliada en la ciudad de Cali, identificada con cédula de ciudadanía No. 66.961.866 expedida en Caicedonia (V), actuando en nombre y representación de la **CONTRALORÍA DEPARTAMENTAL DEL VALLE DEL CAUCA**, en su condición de Contralora Departamental y Representante Legal, elegida por la Asamblea Departamental del Valle del Cauca y debidamente posesionada, de conformidad con el Acta No. 068-2025 de la Sesión Plenaria Ordinaria del 10 de octubre de 2025, en uso de sus facultades constitucionales, legales y administrativas, en especial las conferidas por el literal b) del numeral 3 del artículo 11 de la Ley 80 de 1993, el artículo 94 de la Ley 1474 de 2011 y demás normas concordantes,

por medio de la presente comunica al señor **CESAR FABIÁN COLORADO CORTÉS**, identificado con cédula de ciudadanía No. 1.072.420.300 expedida en La Mesa (Cundinamarca), en calidad de representante legal de **COLCIBER S.A.S.**, identificada con NIT No. 900.859.705-6, la aceptación de la oferta presentada dentro del Proceso de Selección de Mínima Cuantía No. M.C.-006-2026, de conformidad con las siguientes:

CONSIDERACIONES:

Que, de acuerdo con el presupuesto oficial determinado para atender la necesidad de la entidad, la **CONTRALORÍA DEPARTAMENTAL DEL VALLE DEL CAUCA** adelantó el Proceso de Selección de Mínima Cuantía No. M.C.-006-2026, el cual fue publicado en la plataforma SECOP II el 01 de octubre de 2026, de conformidad con las disposiciones aplicables a la modalidad de selección de mínima cuantía.

Que, de conformidad con las disposiciones aplicables a la promoción y limitación de las convocatorias a MIPYMES, la Entidad publicó el 02 de octubre de 2026 el correspondiente aviso en la plataforma SECOP II, mediante el cual se informó que la convocatoria no sería limitada a MIPYMES nacionales, teniendo en cuenta que la solicitud de limitación presentada por INNOVA SOLUCIONES INTEGRADAS fue recibida el 02 de octubre de 2026 a las 12:13 p.m., con posterioridad al plazo establecido en el cronograma del proceso para tal efecto. En consecuencia, por haber sido presentada de manera extemporánea, dicha solicitud no fue tenida en cuenta para efectos de la limitación de la convocatoria a MIPYMES.

Que, de conformidad con el cronograma establecido para el proceso, el 05 de octubre de 2026 se realizó el cierre y apertura de propuestas a través de la plataforma SECOP II, constatándose la recepción de una (1) oferta, presentada por **COLCIBER S.A.S.**, identificada con NIT No. 900.859.705-6, según consta en el Acta de Cierre y Apertura de Propuestas.

Que, mediante Acta No. 02 – Informe de Evaluación del 06 de octubre de 2026, el Comité de Contratación realizó la verificación de los requisitos habilitantes y la evaluación de la oferta presentada, de conformidad con las condiciones establecidas en la Invitación Pública de Mínima Cuantía No. M.C.-006-2026.

Que, como resultado de la evaluación, se determinó que la oferta presentada por **COLCIBER S.A.S.**, identificada con NIT No. **900.859.705-6,** cumple con los requisitos habilitantes, las condiciones y especificaciones técnicas exigidas, y que el valor ofertado se encuentra dentro del presupuesto oficial establecido para el proceso.

Que, de conformidad con lo establecido en el numeral 4 del artículo 2.2.1.2.1.5.2 del Decreto 1082 de 2015, una vez realizada la evaluación de la oferta y verificado el cumplimiento de las condiciones exigidas, procede la aceptación de la oferta presentada por el proponente que resulte habilitado.

Que, durante el término establecido en el cronograma del proceso para la presentación de observaciones al Informe de Evaluación, no se presentaron observaciones, razón por la cual se procede con la aceptación de la oferta presentada por COLCIBER S.A.S., identificada con NIT No. 900.859.705-6, de conformidad con las condiciones establecidas en la Invitación Pública de Mínima Cuantía No. M.C.-006-2026.

RESUELVE:

De acuerdo con lo anterior, se acepta la oferta presentada por el señor **CESAR FABIÁN COLORADO CORTÉS**, identificado con cédula de ciudadanía No. **1.072.420.300**, en su calidad de representante legal de **COLCIBER S.A.S.**, identificada con NIT No. **900.859.705-6**, quien para efectos del presente documento se denominará **EL CONTRATISTA**.

En consecuencia, **EL CONTRATISTA** deberá dar cumplimiento al objeto contractual, de conformidad con las condiciones y exigencias establecidas en los estudios y documentos previos, la Invitación Pública de Mínima Cuantía, sus documentos complementarios, la oferta presentada y demás documentos que hacen parte integral del contrato, en los términos que se establecen a continuación.

1. **OBJETO CONTRATADO:**

ADQUIRIR DOSCIENTAS CINCUENTA (250) LICENCIAS DEL ANTIVIRUS ESET PROTECT COMPLETE, CORRESPONDIENTES A LA RENOVACIÓN DEL LICENCIAMIENTO PARA LA PROTECCIÓN, DETECCIÓN Y ELIMINACIÓN DE VIRUS, TROYANOS, GUSANOS, ADWARE, SPYWARE, PHISHING, ROOTKITS Y ARCHIVOS MALICIOSOS.

1.2 ESPECIFICACIONES TÉCNICAS

EL CONTRATISTA se obliga a entregar los bienes adquiridos con las siguientes especificaciones técnicas:

Las licencias de software antivirus *ESET PROTECT Complete* deben cumplir con las siguientes especificaciones técnicas:

- Consola basada en la nube
- Protección para endpoints
- Sandboxing en la nube
- Cifrado de disco completo
- Protección de apps en la nube

2.2.1 SERVICIO DE SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE ENDPOINTS

La entidad requiere contratar el suministro, implementación, configuración, administración y soporte de una solución integral de seguridad informática para la protección de su infraestructura tecnológica, incluyendo equipos de cómputo, equipos portátiles, dispositivos móviles, servidores, correo electrónico y servicios de almacenamiento y colaboración en la nube.

La solución deberá contar con una plataforma de administración centralizada basada en la nube, que permita gestionar las diferentes capacidades de seguridad desde una única consola, facilitando la implementación, supervisión y administración remota de los dispositivos y servicios protegidos.

El servicio deberá incluir las licencias y funcionalidades necesarias para proporcionar, como mínimo, las siguientes capacidades:

A. PROTECCIÓN CONTRA MALWARE, RANSOMWARE Y AMENAZAS DE DÍA CERO: La solución deberá proporcionar protección multicapa contra malware, ransomware y otras amenazas informáticas, mediante mecanismos de detección y prevención capaces de actuar antes, durante y después de la ejecución de archivos o procesos potencialmente maliciosos.

Deberá incorporar mecanismos de protección frente a amenazas desconocidas y de día cero (0-day), incluyendo análisis de muestras sospechosas mediante sandboxing en la nube, con el propósito de evaluar su comportamiento en un entorno aislado.
La solución deberá incorporar, como mínimo:

- Detección basada en el comportamiento.
- Aprendizaje automático (machine learning).
- Análisis de comportamiento avanzado.
- Análisis estático y dinámico de archivos sospechosos.
- Utilización de información de inteligencia de amenazas.
- Análisis de reputación de archivos.
- Detección de amenazas de día cero (0-day).
- Protección frente a ransomware.
- Protección frente a ataques dirigidos.
- Detección de amenazas persistentes avanzadas.
- Detección y bloqueo de ataques sin archivos (fileless).

B. PROTECCIÓN MULTICAPA DE ENDPOINTS: El servicio deberá proporcionar protección para los equipos de cómputo y equipos portátiles de la entidad mediante una solución de seguridad de múltiples capas.

La solución deberá permitir detectar y bloquear amenazas en las diferentes etapas de un ataque y deberá contar con mecanismos destinados a reducir el riesgo de infección, vulneración de información y ejecución de código malicioso.
La protección deberá contemplar, como mínimo:

- Equipos de escritorio.
- Equipos portátiles.
- Sistemas operativos compatibles con la solución.
- Protección contra malware y ransomware.
- Protección contra ataques dirigidos.
- Protección contra amenazas persistentes avanzadas.
- Detección de ataques sin archivos.
- Protección de la información almacenada en los endpoints.
- Protección de servidores de archivos, cuando se encuentren dentro del alcance de la licencia contratada.

C. PROTECCIÓN DE DISPOSITIVOS MÓVILES: La solución deberá proporcionar mecanismos de seguridad para los dispositivos móviles incluidos dentro del alcance del licenciamiento, permitiendo protegerlos frente a amenazas informáticas y contribuir a la protección de la información institucional.

La administración de estos dispositivos deberá integrarse con la plataforma central de gestión, permitiendo al personal autorizado consultar su estado de protección y administrar las políticas de seguridad correspondientes.

D. PROTECCIÓN DE MICROSOFT 365 Y ONEDRIVE: La solución deberá proporcionar una capa adicional de protección para los servicios de Microsoft 365 utilizados por la entidad, incluyendo el correo electrónico y el almacenamiento de información en la nube.

Deberá contemplar la protección de servicios como Exchange Online, OneDrive, SharePoint Online y Microsoft Teams, de acuerdo con las capacidades contempladas en el licenciamiento contratado.
La solución deberá incorporar mecanismos de:

- Protección antimalware.
- Filtrado de spam.
- Protección Anti-Phishing.
- Análisis de archivos y contenidos potencialmente maliciosos.
- Protección del correo electrónico institucional.
- Protección del almacenamiento en la nube.
- Protección de la información almacenada en OneDrive.

- Detección de amenazas presentes en las aplicaciones de Microsoft 365.
- Protección preventiva frente a amenazas provenientes del correo electrónico.
- Protección frente a malware presente en los servicios y aplicaciones en la nube.

La solución deberá permitir la incorporación y protección automática de los nuevos usuarios de Microsoft 365 que sean incluidos dentro del alcance del servicio. Asimismo, deberá proporcionar visibilidad sobre las detecciones de seguridad y los elementos puestos en cuarentena, permitiendo su consulta y gestión desde la plataforma de administración correspondiente.

E. CIFRADO COMPLETO DE DISCOS: La solución deberá incluir capacidades de cifrado completo de disco (Full Disk Encryption) para proteger la información almacenada en los equipos de la entidad.

El cifrado deberá poder ser administrado de manera centralizada desde la consola de gestión y deberá contemplar equipos con sistemas operativos Windows y macOS, de acuerdo con las plataformas soportadas por la solución.
Como mínimo, deberá permitir:

- Administrar centralizadamente el cifrado de los equipos.
- Cifrar discos completos.
- Cifrar particiones o unidades del sistema.
- Implementar y activar el cifrado de los dispositivos desde la consola de administración.
- Consultar y gestionar el estado del cifrado.
  Proteger la información almacenada en los dispositivos frente a pérdida, robo o acceso no autorizado.
- Contribuir al cumplimiento de las disposiciones aplicables en materia de protección de datos.

F. CONSOLA DE ADMINISTRACIÓN CENTRALIZADA EN LA NUBE: La solución deberá contar con una consola de administración basada en la nube que permita a la entidad gestionar centralizadamente los diferentes componentes de seguridad incluidos en el servicio.

La consola deberá permitir, como mínimo:

- Configurar las políticas de seguridad.
- Implementar las soluciones de protección.
- Administrar los dispositivos protegidos.
- Realizar gestión remota.
- Consultar el estado de protección de los dispositivos.
- Consultar las amenazas detectadas.
- Consultar los usuarios y dispositivos administrados.
- Consultar y gestionar elementos puestos en cuarentena.
- Administrar las capacidades de protección disponibles.
- Gestionar el cifrado de los dispositivos.
- Obtener información consolidada sobre el estado de seguridad de la infraestructura.
- Acceder a la plataforma mediante navegador web.
- Realizar la administración de manera remota y segura.
- Centralizar la gestión de la seguridad desde un único punto.

La plataforma deberá operar bajo un esquema de administración en la nube, sin requerir infraestructura de hardware adicional por parte de la entidad para la operación de la consola de gestión.

G. MONITOREO, ALERTAS Y VISIBILIDAD: El servicio deberá proporcionar mecanismos que permitan al personal autorizado de la entidad realizar seguimiento sobre los eventos y amenazas de seguridad detectados.

La solución deberá permitir consultar, como mínimo:
- Dispositivos protegidos.
- Usuarios administrados.
- Amenazas detectadas.
- Alertas de seguridad.
- Elementos puestos en cuarentena.

- Estado de las protecciones implementadas.
- Estado de los dispositivos.
- Estado del cifrado de los equipos.
- Información relacionada con eventos de seguridad relevantes.

La solución deberá proporcionar mecanismos de notificación frente a la detección de amenazas, de acuerdo con las capacidades disponibles en la plataforma contratada.

H. ADMINISTRACIÓN Y GESTIÓN REMOTA: La solución deberá permitir la administración remota de los componentes de seguridad desde la consola centralizada. El personal autorizado por la entidad deberá poder realizar, según las funcionalidades disponibles en el licenciamiento contratado:

- Consulta del estado de los dispositivos.
- Administración de políticas de seguridad.
- Consulta de amenazas.
- Gestión de elementos en cuarentena.
- Consulta de usuarios y dispositivos.
- Administración de las capacidades de protección.
- Gestión del cifrado de dispositivos.
- Consulta de eventos y alertas de seguridad.

La plataforma deberá permitir el acceso seguro mediante navegador web desde las ubicaciones autorizadas por la entidad.

I. CONDICIONES Y CARACTERÍSTICAS DEL LICENCIAMIENTO

El servicio contratado deberá proporcionar una solución integral de protección que permita a la entidad gestionar centralizadamente la seguridad de sus dispositivos, usuarios, correo electrónico, servicios de Microsoft 365, almacenamiento en OneDrive y demás componentes incluidos en el alcance del licenciamiento.

El contratista deberá garantizar que las funcionalidades suministradas correspondan al licenciamiento contratado de ESET PROTECT Complete, incluyendo las actualizaciones, mantenimiento y soporte asociados a la vigencia de las licencias, de acuerdo con las condiciones establecidas en el contrato.

De igual forma, el servicio deberá contemplar como mínimo las siguientes capacidades:

- Protección multicapa de ENDPOINTS.
- Protección contra malware.
- Protección contra RANSOMWARE.
- Protección contra amenazas de día cero (0-day).
- SANDBOXING en la nube para análisis de amenazas sospechosas.
- Aprendizaje automático y análisis de comportamiento.
- Protección contra ataques sin archivos.
- Protección contra amenazas persistentes avanzadas.
- Protección de dispositivos móviles incluidos en el licenciamiento.
- Protección de servidores de archivos incluidos en el alcance.
- Protección de Microsoft 365.
- Protección de Exchange Online.
- Protección de OneDrive.
- Protección de SharePoint Online y Microsoft Teams, según el alcance y capacidades del licenciamiento.
- Protección Anti-Phishing.
- Filtrado de spam.
- Protección antimalware para servicios en la nube.
- Cifrado completo de disco para Windows y macOS.
- Administración centralizada desde una consola basada en la nube.
- Gestión remota de los dispositivos.
- Visibilidad sobre amenazas, usuarios, dispositivos y elementos en cuarentena.
- Generación de alertas y notificaciones de seguridad.

NOTA: Las licencias no requieren servicio de instalación por parte del contratista, toda vez que su instalación y activación serán realizadas directamente por el personal técnico de la Entidad en los equipos de cómputo relacionados en la Tabla anexa al proceso.

2. OBLIGACIONES CONTRACTUALES

a) Iniciar la ejecución del contrato a través de la plataforma SECOP II, una vez cumplidos los requisitos correspondientes para el inicio de la ejecución contractual.
b) Cumplir con la ejecución del contrato dentro del plazo establecido y de conformidad con las condiciones, características y especificaciones técnicas definidas en el numeral 2.2.1 "ESPECIFICACIONES TÉCNICAS" y demás documentos que hacen parte del proceso de contratación.
c) Suministrar y entregar las 250 licencias del antivirus ESET PROTECT Complete, objeto del contrato, de conformidad con las cantidades, características y condiciones técnicas establecidas por la Entidad.
d) Garantizar que las licencias suministradas correspondan a la solución requerida por la Entidad, se encuentren debidamente licenciadas y permitan su activación y uso durante el período de vigencia contratado.
e) Garantizar durante el período de vigencia de las licencias el acceso a las actualizaciones y mecanismos de protección propios de la solución contratada, de conformidad con las condiciones y alcance del licenciamiento adquirido.
f) Tener en cuenta que la instalación y activación de las licencias en los equipos de cómputo será realizada por el personal técnico de la Entidad, por lo cual el contratista no tendrá a su cargo un servicio de instalación, sin perjuicio del soporte técnico que corresponda al licenciamiento adquirido.
g) Informar oportunamente al supervisor del contrato cualquier circunstancia que pueda afectar o retrasar el cumplimiento de las obligaciones contractuales, indicando las causas y las medidas adoptadas para su atención.
h) Presentar la factura o documento equivalente correspondiente, acompañada de los documentos requeridos para el trámite de pago y de la certificación del supervisor sobre el recibo a satisfacción de las licencias suministradas, de conformidad con las condiciones establecidas en el contrato.
i) Acreditar, para efectos del trámite de pago, el cumplimiento de las obligaciones relacionadas con el pago de aportes al Sistema de Seguridad Social Integral y parafiscales, cuando haya lugar a ello, de conformidad con la normativa vigente.

3. IDENTIFICACIÓN TIPO DE CONTRATO

Atendiendo el objeto a desarrollar, el negocio jurídico de que se trata, se subsume en un de *Contrato de Compraventa.*

4. PLAZO DE EJECUCIÓN

EL CONTRATISTA contará con un plazo máximo de **cinco (5) días hábiles**, contados a partir del cumplimiento de los requisitos establecidos para el inicio de la ejecución del contrato en la plataforma **SECOP II**, para realizar la entrega e instalación de los **ANTIVIRUS**. Los antivirus suministrados deberán contar con una vigencia de **doce (12) meses**, contados a partir de su activación.

5. LUGAR DE PRESTACIÓN DEL SERVICIO

En la ciudad de Cali, en las instalaciones de la Contraloría Departamental del Valle del Cauca, en el Edificio de la Gobernación del Valle del Cauca, Piso 6o. ubicado en la carrera 6ª entre calles 9 y 10.

6. VALOR DEL CONTRATO

El valor del contrato es por DIECINUEVE MILLONES NOVECIENTOS CINCUENTA Y SEIS MIL OCHOCIENTOS TREINTA Y TRES PESOS /MCTE **($19.956.833) M/cte.** IVA incluido.

7. FORMA DE PAGO

LA CONTRALORIA pagará al CONTRATISTA el valor que resulte del presente contrato en un (1) solo pago, dentro de los diez (10) días hábiles siguiente a la radicación por parte del supervisor del contrato en la Subdirección Administrativa para Recursos Físicos y Financieros de la factura comercial, acompañada de la certificación y/o informe de cumplimiento a satisfacción del servicio que expida el supervisor del contrato y de la verificación de la aprobación de la póliza y del cumplimiento por parte del CONTRATISTA de las obligaciones con el Sistema General de Seguridad social (Sistema de salud, riesgos profesionales, pensiones) y Aportes Parafiscales (Cajas de compensación familiar, ICBF y SENA). El pago del valor que se compromete y obliga LA CONTRALORIA se imputará con cargo al presupuesto de gastos de la presente vigencia fiscal- Código de Apropiación Presupuestal No. 2026000135 de fecha septiembre 15 de 2026 - Código de Apropiación 2.1.2.02.02.008.12 – *Servicio de mantenimiento software protección y seguridad*, expedido por la Subdirección Administrativa para los Recursos Físicos y Financieros.

Este valor incluye deducciones adicionales por concepto de estampillas, y descuentos de RETEFUENTE, RETEIVA Y RETEICA.

8. EXIGENCIA DE GARANTÍAS

El contratista se obliga a constituir a su costa y a favor de la Contraloría una garantía que avalará el cumplimiento de las obligaciones surgidas del contrato, constituida a partir de la fecha de suscripción del contrato y que contenga los siguientes amparos:

- **CUMPLIMIENTO**: Por un monto del 10% del contrato y por el término de duración del contrato y cuatro (4) meses más.

9. SUPERVISIÓN

De acuerdo con la Ley 80 de 1993. Ley 1474 de 2011 y manual de contratación de la Contraloría Departamental del Valle se designa al Jefe de la Oficina TIC, como supervisor del cumplimiento del objeto contractual, de conformidad con la invitación y la propuesta por ustedes presentada.

La supervisión de la ejecución y cumplimiento de las obligaciones contraídas por EL CONTRATISTA a favor de la CONTRALORIA DEPARTAMENTAL, estará a cargo de la subdirectora Administrativa para los Recursos Físicos y Financieros.

Serán obligaciones particulares del supervisor las siguientes, sin perjuicio de las demás que le asigne la Ley y demás normas:

a) Velar por el cumplimiento cabal del objeto contractual, dentro del plazo estipulado.
b) Velar por el pago oportuno a la contratista de los valores acordados.
c) Elaborar certificación de cumplimiento a satisfacción en los casos que sean necesario para el desarrollo del contrato o el pago respectivo.
d) Elaborar las actas de iniciación, cortes parciales y liquidación del contrato.
e) Tener en cuenta que toda aclaración con la CONTRATISTA en relación con el Contrato debe ser por escrito.
f) Verificar el pago y afiliación de la seguridad social integral de la contratista.

Conforme establece el artículo 83 de la Ley 1474 de 2011: La supervisión consistirá en el seguimiento técnico, administrativo, financiero, contable y jurídico que, sobre el cumplimiento del objeto del contrato, es ejercida por la misma entidad estatal cuando no requieren conocimientos especializados. Para la

supervisión, la Entidad estatal podrá contratar personal de apoyo, a través de los contratos de prestación de servicios que sean requeridos.

10. CLÁUSULAS EXCEPCIONALES, MULTAS Y CLÁUSULA PENAL PECUNIARIA

De acuerdo con las facultades otorgadas en la ley 80 de 1.993, LA CONTRALORIA goza de las prerrogativas de: INTERPRETACIÓN, MODIFICACIÓN, TERMINACIÓN UNILATERAL Y DE LA CADUCIDAD del contrato o aceptación de la oferta, de conformidad con los Artículos 14, 15, 16, 17 y 18 de la citada Ley.

10.2. CLÁUSULA PENAL PECUNIARIA

En caso de declaratoria de incumplimiento del contrato o aceptación de la oferta o de caducidad de los mismos, el CONTRATISTA pagará a LA CONTRALORIA el equivalente hasta de un diez por ciento (10%) del valor total del contrato que se imputará a los perjuicios que este reciba, lo cual no excluye que LA CONTRALORIA pueda también reclamar perjuicios adicionales.

10.3. SANCIONES Y MULTAS

En el evento de que **EL CONTRATISTA** presente retraso en el cumplimiento del contrato tomando como referencia el plazo que se haya acordado para ello y a su vez LA CONTRALORIA encuentre no procedentes las justificaciones que presente el CONTRATISTA ante esa situación, se impondrá a través de resolución motivada multa equivalente al UNO POR CIENTO (1%) del valor total del contrato sin que estas sobrepasen el diez por ciento (10%) del valor del mismo.

Para estos efectos el Interventor o Supervisor presentará a LA CONTRALORIA un informe motivado (con copia al CONTRATISTA) en donde sustentará la aplicación de la multa respectiva.

LA CONTRALORIA realizará los estudios y análisis del caso y determinará si hay lugar a su aplicación. En ese período, el CONTRATISTA tendrá el derecho a presentar por escrito ante **LA CONTRALORIA** (con copia al Interventor o supervisor) todos los descargos que considere pertinentes, los cuales, de igual forma, serán analizados por LA CONTRALORIA. Todo lo anterior siguiendo el procedimiento establecido en el artículo 86 de la Ley 1474 de 2011.

La cantidad total que por concepto de multas deba pagar el CONTRATISTA a favor de LA CONTRALORIA, podrá ser deducida de cualquier saldo pendiente (actas parciales, acta final, etc.), sin que ello implique que se libera de la responsabilidad de cumplimiento de todos los compromisos adquiridos al firmar o aceptar el contrato.

La aplicación de las multas se entiende sin perjuicio de que, en un momento dado, **LA CONTRALORIA** proceda a declarar la caducidad del Contrato.

LA CONTRALORIA está obligada a enviar a la Cámara de Comercio, la información concemiente al contrato ejecutado, su cuantía, cumplimiento y a las multas y sanciones que en relación con el contrato se hayan impuesto. De igual manera, en el Acta de Liquidación Final del Contrato constará la imposición de tales multas. Cualquier constancia que en el futuro solicite **EL CONTRATISTA,** llevará explícito el monto de las multas que se le hubieren impuesto.

12. CESIÓN DEL CONTRATO

EL CONTRATISTA no podrá ceder en todo o en parte a persona natural o jurídica alguna, los derechos y obligaciones inherentes al presente contrato, salvo autorización previa y expresa de la entidad contratante, en todo caso se atenderá lo dispuesto en el Artículo 41, Inciso 3° de la Ley 80 de 1993.

El contratista acepta que, en el evento de surgir diferencias relacionadas con el desarrollo y la ejecución del contrato, o referentes a actos de la Administración que alteren la relación contractual, las partes acudirán al empleo de los mecanismos de solución de controversias contractuales previsto en la Ley 80 de 1993, demás normas concordantes y de conformidad con los procedimientos legales, y el manual de contratación de la entidad.

Contraloría
Departamental del Valle del Cauca

Para todos los efectos de ejecución del objeto contractual, el domicilio contractual es el municipio de Cali y para las correspondientes notificaciones se tendrán en cuenta las siguientes direcciones: La Contraloría, en el Edificio San Francisco Gobernación del Valle 6 piso, ubicado en la carrera 6 entre calles 9 y 10 de la ciudad de Cali, El Contratista, en Lt San Francisco Of B21 Et 1 Centro Empresarial Metropolitano Ph en Cota, Cundinamarca.

LINA MARCELA VASQUEZ VARGAS
Contralora Departamental del Valle del Cauca

	Nombre	Cargo	Firma
Proyectó	Ingrid Julieth Rivera Pino	Profesional Universitario	
Revisó y aprobó:	Diana Lucía Patiño López	Jefe Oficina Jurídica	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			

CODIGO: M1P2-03	VERSION: 1.0