Dependencia que requiere el servicio	Dirección Desarrollo Tecnológico

De conformidad con lo establecido en el numeral 12 del artículo 25 de la Ley 80 de 1993, la Ley 1150 de 2007 y en especial lo establecido por los artículos 2.2.1.1.2.1.1 y 2.2.1.2.1.4.9.del Decreto 1082 de 2015, se realiza el presente estudio previo.

1. LA DESCRIPCIÓN DE LA NECESIDAD QUE LA CONTRALORÍA DISTRITAL DE MEDELLÍN PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN:

La Contraloría Distrital de Medellín, en cumplimiento de las funciones constitucionales y legales que le corresponden como organismo de control fiscal territorial, *debe garantizar la disponibilidad, integridad, confidencialidad y autenticidad de la información* que administra, así como la continuidad y seguridad de los servicios digitales que soportan sus procesos misionales, estratégicos y de apoyo. Lo anterior se desprende de los principios de la función administrativa previstos en el artículo 209 de la Constitución Política y de los lineamientos de Gobierno Digital, Seguridad de la Información y Control Interno aplicables a las entidades públicas.

Para el cumplimiento de su misión, la Entidad dispone de portales web, aplicaciones, y servicios institucionales accesibles a través de internet, que permiten el intercambio permanente de información con ciudadanos, sujetos de control, servidores públicos y demás grupos de interés. Por ello, es indispensable que las comunicaciones realizadas mediante estos servicios se efectúen por canales confiables y protegidos frente a riesgos de interceptación, alteración, suplantación o acceso no autorizado.

La ausencia, expiración o inadecuada gestión de los mecanismos de protección asociados a estos servicios puede generar pérdida de confianza de los usuarios, exposición de información durante su transmisión, indisponibilidad de servicios institucionales, advertencias de seguridad en los navegadores y riesgos de suplantación de identidad digital, con impacto en la operación y en la imagen de la Entidad.

Un certificado digital SSL/TLS (Secure Sockets Layer / Transport Layer Security) permite a un sitio web o sistema de información demostrar ante los navegadores y los usuarios que el dominio pertenece realmente a la entidad que afirma ser su titular, lo que ayuda a prevenir la suplantación o clonación de sitios. Así mismo, garantiza que la información transmitida entre el navegador del usuario y el servidor de la Entidad viaje cifrada, evitando su interceptación o alteración por terceros. Gracias a ello, los sitios se identifican como seguros mediante el candado y el prefijo “https://”, en lugar de mostrar advertencias de conexión no segura.

En cumplimiento de las políticas de Gobierno Digital y de seguridad de la información definidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Entidad requiere mantener vigentes estos certificados sobre el dominio institucional cdm.gov.co y sus subdominios, que respaldan tanto el portal web público como los sistemas de información utilizados por los servidores en el desarrollo de sus funciones.

Con fundamento en el análisis realizado por la Dirección de Desarrollo Tecnológico, se identificó la necesidad de contar con certificados digitales SSL/TLS emitidos bajo estándares de reconocimiento internacional para los dominios y subdominios institucionales, que garanticen la autenticidad de los servicios, la protección de la información transmitida y el adecuado funcionamiento de los mecanismos de confianza exigidos en los entornos digitales actuales.

La Entidad cuenta con certificados vigentes, adquiridos mediante el contrato MC0522024 suscrito con Camerfirma Colombia S.A.S. en noviembre y diciembre de 2024, cuya fecha de vencimiento es próxima. Los dominios están distribuidos en dos certificados multidominio (SAN) con niveles de validación diferentes: el primero, de nivel EV, incluye isolucion.cdm.gov.co, www.cdm.gov.co, sunificado.cdm.gov.co y mercurio.cdm.gov.co; el segundo, de nivel OV, incluye academia.cdm.gov.co, tech.cdm.gov.co e intranet.cdm.gov.co. Esta coexistencia, heredada de renovaciones anteriores, no responde a una necesidad funcional ni a un requerimiento diferencial de seguridad.

En los últimos años, las autoridades certificadoras, los fabricantes de navegadores y las organizaciones que integran los ecosistemas globales de certificación digital han fortalecido los requisitos técnicos y de validación de los certificados SSL/TLS. Como consecuencia, la gestión de estos certificados dejó de ser una simple actividad de soporte tecnológico y pasó a ser un componente esencial de la estrategia de ciberseguridad y de la continuidad operativa de los servicios digitales.

En ese marco, el CA/Browser Forum, organismo que reúne a las principales autoridades certificadoras del mundo y a los desarrolladores de los navegadores más utilizados entre ellos Google, Apple, Mozilla y Microsoft, aprobó la iniciativa denominada Ballot SC-081v3. Esta establece un cronograma de reducción progresiva de la vigencia máxima de los certificados SSL/TLS emitidos en cualquier país y por cualquier proveedor. Por esta razón, el esquema de actualización mediante una única adquisición anual, utilizado hasta ahora por la Entidad, dejó de ser viable.

La reducción progresiva de las vigencias se presenta a continuación:

Fecha	**Vigencia máxima**
Hasta marzo de 2026	398 días (aprox. 13 meses)

Desde el 15 de marzo de 2026	200 días (aprox. 6,5 meses)
Desde el 15 de marzo de 2027	100 días (aprox. 3,3 meses)
Desde el 15 de marzo de 2029	47 días (aprox. 1,5 meses)

Esta medida responde a consideraciones de seguridad informática, ya que, cuanto menor es la vigencia de un certificado, menor es el riesgo de que continúe utilizándose con información desactualizada o con una clave privada comprometida que no haya sido detectada oportunamente.

La Entidad ya no puede planificar una única actualización anual de sus certificados. Con vigencias máximas de 200, 100 y, desde 2029, 47 días, un mismo certificado podría requerir hasta ocho actualizaciones al año. Este escenario genera dos riesgos que deben gestionarse de manera preventiva:

Aumenta la probabilidad de que un certificado expire sin ser renovado oportunamente, especialmente si los procesos dependen de controles manuales, con afectación dela disponibilidad de los sitios o sistemas institucionales y advertencias de seguridad para los usuarios.

Se incrementa la carga operativa asociada a la generación, validación, instalación y seguimiento de cada actualización, actividades que antes se realizaban una vez al año.

Por ello, la tendencia internacional consiste en incorporar mecanismos de automatización que permitan gestionar las actualizaciones de forma segura, oportuna y continua, reduciendo la dependencia de intervenciones manuales

Para efectos de este estudio, se precisan dos clasificaciones que se combinan al definir un certificado:

Por nivel de validación de identidad:

• **DV (Domain Validation):** valida únicamente que quien lo solicita controla el dominio. Es el nivel más básico, de emisión rápida, usado típicamente en sitios informativos.

• **OV (Organization Validation):** valida además que la entidad solicitante existe legalmente, mediante verificación de su documentación institucional. Es un nivel plenamente adecuado para entidades públicas.

• **EV (Extended Validation):** es el nivel de validación más riguroso (verificación legal, física y operativa de la organización). Sin embargo, los navegadores más usados (Chrome, Firefox, Edge) dejaron de mostrar diferencias visuales entre un certificado EV y uno OV: antes el EV

mostraba una barra verde con el nombre de la entidad junto al candado, y hoy ambos se ven igual para quien navega el sitio.

Por cobertura de dominios:

• Dominio único (single domain): cubre un solo nombre de dominio.

•Multidominio (SAN, Subject Alternative Name): permite incluir varios dominios distintos en un mismo certificado, pero cada uno debe enumerarse manualmente y validarse de forma independiente. Si un dominio queda mal escrito, omitido o mal validado, queda sin protección, sin que necesariamente se advierta de inmediato.

• Wildcard (comodín): un solo certificado, identificado con un asterisco (por ejemplo, *.cdm.gov.co), que cubre automáticamente todos los subdominios de primer nivel del dominio institucional, actuales y futuros, sin necesidad de enumerarlos ni de tramitar un certificado nuevo para cada subdominio que se habilite.

Las reglas del CA/Browser Forum no permiten emitir certificados EV bajo la modalidad Wildcard, pues este nivel exige verificar individualmente la titularidad de cada dominio incluido, requisito incompatible con el modelo comodín. Por lo tanto, es necesario estandarizar los certificados de la Entidad en nivel OV. Este ofrece una validación adecuada para una entidad pública, evita los costos adicionales de los certificados EV, que no representan una diferencia perceptible para los usuarios, y permite adoptar un esquema Wildcard que simplifica la administración y actualización de los dominios institucionales.

Frente al esquema de actualizaciones periódicas que impone el nuevo régimen internacional, se evaluaron dos alternativas. La primera consistía en mantener certificados multidominio (SAN) segmentados, incorporando explícitamente cada dominio institucional. La segunda contemplaba un único certificado Wildcard OV (*.cdm.gov.co), complementado con el dominio raíz (cdm.gov.co) y su variante www (www.cdm.gov.co) como SAN, pues un certificado Wildcard no protege automáticamente ni el dominio raíz ni su variante www.

Se consideró más conveniente la segunda alternativa, por las siguientes razones:

• Reduce a una sola validación de dominio (DCV) un procedimiento que, en un esquema segmentado, tendría que repetirse para cada dominio y en cada ciclo de actualización.

• Elimina el riesgo, frecuente en configuraciones multidominio, de que algún dominio quede omitido, mal incluido o con inconsistencias en su validación.

• Cubre automáticamente los nuevos subdominios que la Entidad habilite, en concordancia con las iniciativas y desarrollos previstos en el Plan Estratégico Institucional, sin gestionar certificados o SAN adicionales.

En consecuencia, la Contraloría Distrital de Medellín requiere contratar la adquisición y actualización de un (1) certificado digital SSL/TLS tipo OV, en modalidad Wildcard con SAN, para sus dominios y subdominios institucionales, con cobertura de dos (2) años que incluya las actualizaciones necesarias conforme a las vigencias máximas permitidas. Con ello se mantienen vigentes los mecanismos de seguridad implementados, se garantiza la continuidad de los servicios digitales y se atienden las exigencias técnicas y de confianza actuales.

2. EL OBJETO A CONTRATAR, CON SUS ESPECIFICACIONES, LAS AUTORIZACIONES, PERMISOS, LICENCIAS REQUERIDAS PARA SU EJECUCIÓN Y CUANDO EL CONTRATO INCLUYE DISEÑO Y CONSTRUCCIÓN, LOS DOCUMENTOS TÉCNICOS PARA EL DESARROLLO DEL PROYECTO:

a.) Objeto del contrato.

Adquisición de un (1) certificado digital SSL/TLS OV Wildcard con SAN, con cobertura de dos (2) años que incluye actualizaciones, instalación y soporte técnico, para los dominios y subdominios institucionales de la Contraloría Distrital de Medellín.

Clasificación UNSPSC: se relacionan a continuación el código de Producto principal y los códigos complementarios identificados, cada uno con su respectiva cadena de clasificación (Segmento / Familia / Clase / Producto):

Códigos UNSPSC:

Segmento	43000000
Familia	43230000
Clase	43233200
Nombre producto	Software de gestión de contenidos

Segmento	43000000
Familia	43230000
Clase	43233200
Producto	43233201
Nombre producto	Software de servidor de autenticación

Segmento	43000000
Familia	43230000
Clase	43233200
Producto	43233205

Nombre producto	Software de seguridad de transacciones y de protección contra virus

Segmento	81000000
Familia	81110000
Clase	81112200
Nombre	Mantenimiento y soporte de software

b.) Especificaciones técnicas mínimas exigidas

El alcance del objeto a ejecutar comprende la emisión inicial de un (1) certificado digital y las actualizaciones del mismo durante los dos (2) años de cobertura del servicio, con las siguientes características técnicas mínimas:

Característica	**Especificación**
Cantidad	Un (1) certificado digital (no se requieren certificados adicionales; el dominio raíz y www quedan cubiertos como SAN dentro del mismo certificado)
Nivel de validación	OV (Organization Validation) - validación de la organización, apropiada para una entidad pública
Tipo de cobertura	Wildcard, con inclusión expresa de Subject Alternative Names (SAN)
Common Name (CN)	*.cdm.gov.co - cubre automáticamente los subdominios de primer nivel actuales y futuros del dominio institucional, sin necesidad de solicitar un SAN nuevo por cada uno
Subject Alternative Names (SAN) adicionales	Debe incluirse expresamente, al momento de generar la solicitud de certificado (CSR), el dominio raíz cdm.gov.co y el subdominio www.cdm.gov.co como Alternative Names, dado que un certificado Wildcard no cubre automáticamente el dominio raíz
Generación del CSR y custodia de la clave privada	La Contraloría Distrital de Medellín generará la solicitud de firma de certificado (CSR) y conservará bajo su exclusiva custodia la clave privada correspondiente; el proveedor no tendrá acceso a la clave privada en ningún momento del proceso de emisión o actualización.
Algoritmo y longitud de clave	RSA 2048 bits (mínimo) o superior, cifrado SHA-256

Método de validación de dominio (DCV)	CNAME, con soporte de delegación persistente que permita automatizar las validaciones en cada actualización, sin requerir intervención manual repetida de la Entidad
Entrega de la cadena de certificación	El proveedor debe entregar el certificado junto con la cadena completa de certificación (certificados intermedios y raíz) en los formatos requeridos para su instalación en los servidores de la Entidad (.crt, .pem, .p7b), sin costo adicional.
Duración del contrato	Diez (10) días calendario, conforme al plazo de ejecución y legalización propio de la modalidad de mínima cuantía.
Cobertura del servicio	Dos (2) años, contados desde la entrega inicial del certificado, cubriendo todas las actualizaciones que se realizaran cada 199 días y se estima que sean 4 durante los 2 años
Vigencia por emisión	La máxima vigencia permitida al momento de cada emisión conforme al cronograma del CA/Browser Forum (actualmente 200 días, con reducciones posteriores a 100 y 47 días)
Actualizaciones	Ilimitadas y sin costo adicional durante los dos (2) años de cobertura del servicio, activándose automáticamente al vencimiento de cada período de vigencia
Alertas de vencimiento	El proveedor debe remitir notificaciones automáticas de vencimiento próximo del certificado a los correos institucionales que indique la Entidad, con una anticipación mínima de treinta (30), quince (15) y cinco (5) días calendario antes de cada vencimiento, sin costo adicional.
Tiempo de atención de actualizaciones y soporte	Las solicitudes de actualización y los requerimientos de soporte técnico deberán atenderse dentro de un plazo máximo de un (1) día hábil contado desde su radicación, con cargo a la bolsa de soporte técnico contemplada en el presente estudio.
Garantía / póliza de cobertura	El proveedor debe indicar expresamente el valor de la póliza de cobertura asociada al certificado, con vigencia acorde a los dos (2) años de cobertura del servicio

El proveedor deberá indicar expresamente, en su propuesta, el nivel de validación, el tipo de cobertura (Wildcard + SAN) y confirmar el soporte de delegación persistente de DCV, evitando ambigüedad sobre el alcance técnico del certificado ofertado.

Nota técnica: al momento de generar la solicitud de firma de certificado (CSR), el campo "Common Name" debe diligenciarse como *.cdm.gov.co, y el campo "Alternative Names" (Subject Alternative Names) debe incluir tanto cdm.gov.co (dominio raíz) como www.cdm.gov.co, para que ambos queden protegidos por el certificado.

Entregables

- Certificado digital SSL/TLS emitido, instalado y verificado en los servicios correspondientes.
- Constancia o soporte de emisión del certificado, indicando CN, SAN, nivel de validación y vigencia.
- Soporte de configuración inicial y validación de la cadena de certificación.
- Confirmación expresa del método de DCV utilizado y su soporte de delegación persistente para renovaciones futuras.

c.) Plazo y sitio de entrega:

El término estimado de duración del contrato será de diez (10) días calendario contados a partir de la legalización del contrato y de la fecha de inicio registrada en la plataforma del SECOP II previa aprobación de las garantías exigidas por la Contraloría Distrital de Medellín.

La entrega, instalación y soporte de configuración se realizará de manera remota, mediante la validación del dominio (DCV) y la configuración directa en los servidores institucionales de la Contraloría Distrital de Medellín bajo la coordinación de la Dirección de Desarrollo Tecnológico.

3. LA MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y SU JUSTIFICACIÓN, INCLUYENDO LOS FUNDAMENTOS JURÍDICOS:

De conformidad con lo establecido en el numeral 5 del artículo 2 de la Ley 1150 de 2007, modificado por el artículo 94 de la Ley 1474 de 2011, y en las disposiciones reglamentarias contenidas en la Subsección 5 de la Sección 1 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, la modalidad de selección de mínima cuantía procede para

la adquisición de bienes, obras y servicios cuyo valor no exceda el diez por ciento (10%) de la menor cuantía de la entidad estatal.

Una vez realizado el análisis de la necesidad, el estudio del sector y la estimación del presupuesto oficial, se determinó que el valor estimado para la adquisición y actualización de los certificados digitales SSL/TLS requeridos por la Contraloría Distrital de Medellín se encuentra dentro del límite legal previsto para la contratación mediante mínima cuantía, razón por la cual esta modalidad resulta procedente para la selección del contratista.

Previamente a la definición de la modalidad de selección, la Entidad verificó en la Tienda Virtual del Estado Colombiano, administrada por Colombia Compra Eficiente, la existencia de instrumentos de agregación de demanda aplicables a la adquisición de los certificados digitales SSL/TLS requeridos.

Como resultado de dicha revisión, se evidenció que el Acuerdo Marco de Precios CCE-309-AMP-2022 denominado *"Productos y Servicios Electrónicos y Digitales de Confianza"* contemplaba dentro de su alcance la adquisición de certificados digitales SSL en las modalidades DV, OV y EV. No obstante, dicho Acuerdo Marco se encuentra cerrado para la generación de nuevas órdenes de compra desde el 27 de diciembre de 2025, permitiéndose únicamente la ejecución de aquellas expedidas con anterioridad a esta fecha y hasta el 27 de diciembre de 2026.

De igual manera, se verificó el Acuerdo Marco de Servicios de Conectividad IV, encontrándose que este no incluye dentro de su catálogo la adquisición de certificados digitales SSL/TLS para dominios institucionales. Aunque contempla la alternativa denominada "VPN Client to Site SSL", esta corresponde a un servicio de conectividad remota que emplea el protocolo SSL como mecanismo de cifrado para el establecimiento de túneles VPN y no a un servicio de certificación digital de dominios, por lo que no satisface la necesidad que se pretende contratar.

En consecuencia, a la fecha de elaboración del presente estudio no existe un Acuerdo Marco de Precios o Instrumento de Agregación de Demanda vigente y aplicable que permita satisfacer la necesidad identificada, razón por la cual la Contraloría Distrital de Medellín debe adelantar un procedimiento de selección propio conforme a las disposiciones aplicables a la modalidad de mínima cuantía.

En virtud de lo expuesto, la Contraloría Distrital de Medellín adelantará el presente proceso contractual mediante la modalidad de Selección de Mínima Cuantía, observando los principios de transparencia, economía, responsabilidad, publicidad y selección objetiva que rigen la contratación estatal, adjudicando el contrato al oferente que cumpla los requisitos habilitantes exigidos y presente la oferta económica de menor valor, de conformidad con las condiciones establecidas en la invitación pública.

Se deja constancia de que el presupuesto oficial estimado para el presente proceso contractual corresponde a una cuantía inferior al diez por ciento (10%) de la menor cuantía de la Contraloría Distrital de Medellín para la vigencia fiscal 2026, circunstancia que habilita legalmente la utilización de la modalidad de selección de mínima cuantía.

4. VALOR ESTIMADO DEL CONTRATO Y LA JUSTIFICACIÓN DEL MISMO:

Análisis del Sector – Estudio del Mercado:

En cumplimiento de lo establecido en la Guía para la Elaboración de Estudios del Sector de Colombia Compra Eficiente, la Entidad realizó el análisis del mercado con el fin de identificar las condiciones técnicas, económicas y comerciales del servicio requerido, correspondiente a la actualización los certificados SSL, en esta ocasión en la modalidad wildcard con dominios adicionales (SAN).

Aspectos generales del mercado

Contexto económico. Para analizar las variables del sector económico donde se ubica el servicio objeto de esta contratación, es necesario en primera instancia identificar la correspondencia entre los servicios y un estándar referente, que para este caso se utilizará la Clasificación Industrial Internacional Uniforme CIIU Revisión 4, adaptada para Colombia CIIU Rev. 4 A. C.

En esta clasificación publicada por el Departamento Administrativo Nacional de Estadística (DANE) se ubicó la actividad económica con la siguiente estructura clasificatoria:

SECCIÓN ACTIVIDAD ECONÓMICA	DIVISIÓN	GRUPO	CLASE
J6209 Otras actividades de tecnologías de información y actividades de servicios.	62	620	6209

J6311 Procesamiento de datos, alojamiento (hosting) y actividades relacionadas.	63	631	6311
J4651 Comercio al por mayor de computadores, equipos periféricos y programas de informática.	46	465	4651

El servicio objeto del contrato corresponde a la adquisición y actualización de un (1) certificado digital de sitio seguro tipo Secure Site Ov (SSL-OV), en modalidad wildcard con dominios adicionales (SAN), para los dominios y subdominios institucionales de la Contraloría Distrital de Medellín.

Corresponde a un servicio especializado de seguridad informática que permite fortalecer la protección de los activos digitales institucionales, garantizando la autenticidad de los dominios y subdominios de la Entidad, el cifrado de las comunicaciones y el cumplimiento de los estándares de seguridad exigidos por los navegadores, sistemas operativos y demás plataformas tecnológicas vigentes.

En el mercado nacional existe pluralidad de oferentes con capacidad administrativa, operativa, financiera y técnica para suministrar, implementar y brindar soporte para este tipo de certificados digitales; dichos servicios son ofrecidos por empresas especializadas en seguridad informática, infraestructura tecnológica y certificación digital, lo que permite evidenciar la existencia de condiciones de competencia suficientes para adelantar el respectivo proceso de contratación.

Entre las principales características de este mercado se destacan:

- Especialización técnica: Los productos y servicios son suministrados por autoridades certificadoras o por distribuidores autorizados que cuentan con conocimientos especializados en infraestructura de claves públicas (PKI), criptografía, seguridad informática y administración de certificados digitales.
- Estándares internacionales: Los certificados SSL/TLS son emitidos bajo estándares y prácticas reconocidas internacionalmente, garantizando su aceptación por los principales navegadores web, sistemas operativos y plataformas tecnológicas.
- Pluralidad de oferentes: Existe una oferta amplia de proveedores y distribuidores autorizados de diferentes marcas y autoridades certificadoras, lo que favorece la libre competencia y la concurrencia de oferentes en los procesos de contratación.

- Mercado altamente competitivo: Los proveedores compiten principalmente en aspectos como precio, soporte técnico, tiempos de emisión, acompañamiento durante la validación, servicios de instalación y garantías asociadas al certificado.
- Actualización permanente: Debido a la evolución constante de las amenazas cibernéticas y de los estándares tecnológicos, los productos ofrecidos en este mercado requieren actualización continua para mantener los niveles de seguridad exigidos por la industria.
- Interoperabilidad tecnológica: Los certificados disponibles en el mercado deben garantizar compatibilidad con diferentes servidores web, aplicaciones, sistemas operativos, dispositivos móviles y navegadores utilizados por los usuarios.
- Demanda recurrente: Se trata de una necesidad permanente para entidades públicas y privadas que ofrecen servicios digitales, dado que los certificados cuentan con vigencia limitada y deben renovarse periódicamente para mantener la seguridad y continuidad de los servicios.
- Bajas barreras de participación comercial: Aunque la emisión de certificados corresponde a autoridades certificadoras reconocidas, existe un número significativo de distribuidores, integradores y partners tecnológicos que pueden comercializar estas soluciones y prestar servicios asociados de soporte e implementación.

Aspecto técnico

Las soluciones disponibles en el mercado para este tipo de requerimientos presentan características homogéneas en cuanto a su finalidad, orientada a garantizar:

- Validación de identidad organizacional (OV).
- Cifrado de la información mediante protocolos SSL/TLS.
- Protección de dominios y subdominios mediante certificados Wildcard.
- Inclusión de dominios adicionales a través de SAN.
- Compatibilidad con los principales navegadores y sistemas operativos.
- Emisión y validación bajo estándares internacionales de seguridad.
- Soporte técnico especializado para instalación y administración del certificado.
- Actualización periódica de conformidad con las condiciones establecidas por la autoridad certificadora.

Regulatorio

Es importante precisar que, en Colombia, no existe una norma que ordene expresamente a todas las entidades públicas adquirir un certificado SSL/TLS específico (por ejemplo, SSL OV Wildcard). Sin embargo, sí existe un marco normativo y de política pública que obliga a las entidades a implementar controles de seguridad digital y protección de la información, dentro de los cuales los certificados SSL/TLS constituyen una medida técnica ampliamente aceptada y necesaria para proteger los servicios web institucionales.

Normas como el Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC), el cual establece la Política de Gobierno Digital y dispone que las entidades públicas deben implementar medidas de seguridad y privacidad de la información para proteger sus servicios digitales y generar confianza en el entorno digital. Por su parte el Decreto 338 de 2022 fortaleció la gobernanza de la seguridad digital en Colombia y estableció lineamientos generales para la gestión de riesgos de seguridad digital en las entidades públicas; buscando con esta norma que las entidades adopten medidas para proteger la infraestructura tecnológica y los servicios digitales frente a amenazas y vulnerabilidades cibernéticas.

a) Aspecto de la Oferta

El mercado de certificados digitales SSL/TLS se encuentra ampliamente desarrollado tanto a nivel internacional como nacional, existiendo una pluralidad de fabricantes, autoridades certificadoras y proveedores autorizados que ofrecen soluciones de validación organizacional (OV), certificados tipo Wildcard y certificados con dominios adicionales (SAN). Para el caso de Colombia existe una oferta suficiente de empresas especializadas en tecnologías de la información, seguridad informática, infraestructura tecnológica y comercialización de soluciones de ciberseguridad, que cuentan con la capacidad administrativa, técnica, operativa y financiera para suministrar este tipo de certificados, así como para brindar acompañamiento durante los procesos de validación, emisión, instalación, soporte y actualización.

La existencia de diversos distribuidores autorizados y partners tecnológicos permite identificar condiciones de competencia adecuadas para satisfacer la necesidad de la Entidad, sin que se evidencien barreras significativas de acceso al mercado ni situaciones que limiten la pluralidad de oferentes.

b) Aspecto de la Demanda

Modelo de Abastecimiento Estratégico de Colombia Compra Eficiente

Acorde al objeto contractual y a las especificaciones técnicas, el servicios se clasifica en los siguientes códigos:

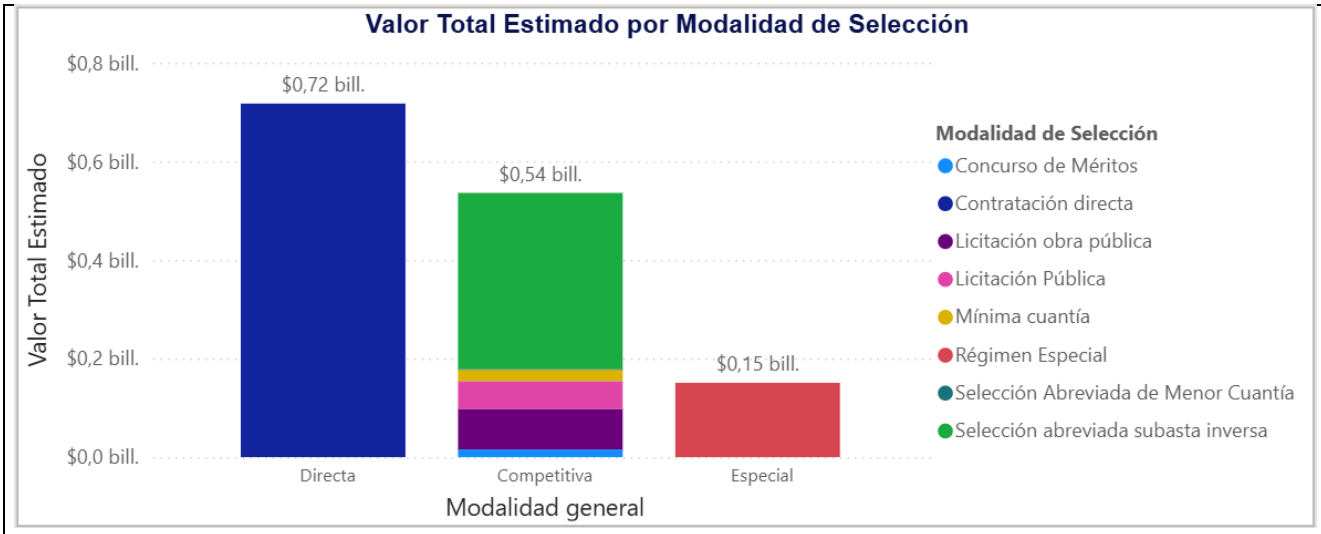
- Código UNSPSC principal – 43233201 - Software de servidor de autenticación.
- Código UNSPSC complementario 1 – 43233205 - Software de seguridad de transacciones y de protección contra virus.
- Código UNSPSC complementario 2 – 81112200 - Mantenimiento y soporte de software (soporte técnico y actualizaciones periódicas del certificado).

En base a estos códigos se realiza el análisis de la demanda consultando el modelo de abastecimiento de Colombia Compra Eficiente, a través de la herramienta de análisis de demanda; arrojando los siguientes resultados:

- Bienes y servicios 432332 y 811122: para el objeto de estudio se reportaron a nivel nacional un total de 2493 contratos por valor de $1.404.264.172.415 entre enero de 2025 y el 9 de agosto de 2026.

Comportamiento contratación por bienes y servicios de UNSPSC

Año	2025			2026			Total		
Clasificador de Bienes y Servicios - Familia	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación
8111 - Servicios informáticos	**2066**	**$770.897.468.599**	**54,90%**	**1498**	**$411.196.240.423**	**29,28%**	**3564**	**$1.182.093.709.022**	**84,18%**
811122 - Mantenimiento y soporte de software	2066	$770.897.468.599	54,90%	1498	$411.196.240.423	29,28%	3564	$1.182.093.709.022	84,18%
4323 - Software	**427**	**$165.022.808.260**	**11,75%**	**270**	**$57.147.655.133**	**4,07%**	**697**	**$222.170.463.393**	**15,82%**
432332 - Software de seguridad y protección	427	$165.022.808.260	11,75%	270	$57.147.655.133	4,07%	697	$222.170.463.393	15,82%
Total	**2493**	**$935.920.276.859**	**66,65%**	**1766**	**$468.343.895.556**	**33,35%**	**4259**	**$1.404.264.172.415**	**100,00%**


Valor Total Estimado por Modalidad de Selección
$0,8 bill.
$0,6 bill.
$0,4 bill.
$0,2 bill.
$0,0 bill.
Valor Total Estimado
$0,72 bill.
$0,54 bill.
$0,15 bill.
Directa
Competitiva
Especial
Modalidad general
Modalidad de Selección
Concurso de Méritos
Contratación directa
Licitación obra pública
Licitación Pública
Mínima cuantía
Régimen Especial
Selección Abreviada de Menor Cuantía
Selección abreviada subasta inversa


Número de Contratos por Proveedores
Proveedores
CAMERFIRMA
CERTICAMARA SA
Oracle Colombia Ltda
DIGITAL WARE SAS
Gestión de Seguridad Electrónica SAS
SISTEMAS ARIES SAS
SINFA SISTEMA DE INFORMACIÓN FINANCIERO Y ADMI...
Gestión de Seguridad Electrónica SA
HAS SQL SAS
SYSMAN SAS
INTEGRAL V6 SAS
COOPERATIVA INTEGRAL DE TRABAJO ASOCIADO LIMIT...
0
100
Número de Contratos

Comportamiento contratación por bienes y servicios de UNSPSC

Año	2025			2026			Total		
Clasificador de Bienes y Servicios - Familia	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación
8111 - Servicios informáticos	**2066**	**$770.897.468.599**	**54,90%**	**1498**	**$411.196.240.423**	**29,28%**	**3564**	**$1.182.093.709.022**	**84,18%**
811122 - Mantenimiento y soporte de software	2066	$770.897.468.599	54,90%	1498	$411.196.240.423	29,28%	3564	$1.182.093.709.022	84,18%
4323 - Software	**427**	**$165.022.808.260**	**11,75%**	**270**	**$57.147.655.133**	**4,07%**	**697**	**$222.170.463.393**	**15,82%**
432332 - Software de seguridad y protección	427	$165.022.808.260	11,75%	270	$57.147.655.133	4,07%	697	$222.170.463.393	15,82%
Total	**2493**	**$935.920.276.859**	**66,65%**	**1766**	**$468.343.895.556**	**33,35%**	**4259**	**$1.404.264.172.415**	**100,00%**

Del análisis de la información presentada se observa que la clase 811122 – Mantenimiento y soporte informático registró durante la vigencia 2025 un total de 2.066 contratos, por valor de $770.897.468.599. Por su parte, para la vigencia 2026, con corte al 9 de agosto, se han suscrito 1.497 contratos por $411.196.240.423.

Al realizar un análisis comparativo basado en el promedio diario de contratación, se evidencia que durante 2025 se celebraron aproximadamente 5,6 contratos por día, mientras que en 2026 dicho indicador asciende a 6,7 contratos por día, lo que refleja una tendencia de crecimiento en la demanda de este tipo de servicios.

Este comportamiento podría estar asociado al fortalecimiento de las estrategias de transformación digital, mantenimiento de la infraestructura tecnológica y adopción de medidas de ciberseguridad por parte de las entidades públicas, en respuesta a la necesidad de proteger sus sistemas de información, garantizar la continuidad de los servicios digitales y atender las recomendaciones emitidas por las áreas de seguridad de la información y seguridad digital.

SECOP II

Con el fin de identificar la forma en que otras entidades adquieren este servicio, se revisaron procesos publicados en la plataforma SECOP II con objeto similar, obteniendo la siguiente información:

Procesos de referencia SECOP II – 2026

Entidad	Referencia del Proceso	Descripción del Procedimiento	Fase Selección	Precio Base	Modalidad de Contratación	Duración
Instituto Nacional para Sordos	MC-016-2026	Adquisición de certificado digital SSL Wildcard y soporte técnico para los dominios y subdominios de los diferentes portales web del INSOR.	08/25/2026	$ 2.427.175	Mínima cuantía	30 días

Acueducto Metropolitano de Bucaramanga S.A. E.S.P.	OC-5765	Adquisición de certificado SSL Wildcard para los servicios web del dominio amb.com.co por un año.	6/03/2026	$ 2.387.718	Contratación régimen especial	90 días
E.S.E Hospital del Rosario	CPS 238 2026	Adquirir, instalar, configurar e implementar un certificado SSL para el aseguramiento de las comunicaciones digitales de la E.S.E. Hospital del Rosario de Campoalegre Huila.	05/14/2026	$ 1.785.000	Contratación régimen especial	14
Unidad AESPE	SPE-SDT-MC-004-2026	500025 Adquisición de certificados digitales de sitio seguro SSL para sitios web de la Unidad Administrativa Especial del Servicio Público de Empleo.	5/08/2026	$ 3.867.705	Mínima cuantía	15 días
Caja de Sueldos de Retiro de la Policía Nacional	INV005-26	Adquisición del certificado digital de seguridad del portal web de CASUR (SSL).	3/12/2026	$ 2.895.000	Mínima cuantía	60 días
Agencia Nacional del Espectro	MC-120-2026	Adquirir certificados digitales de: firma digital función pública (dispositivos criptográficos- token), firma digital de persona jurídica - facturación electrónica, y de Wilcard SSL OV para el dominio y los subdominios (*.ane.gov.co).	02/18/2026	$ 5.402.600	Mínima cuantía	10 días
Contraloría de Bogotá	CB-PMINC-001-2026	Adquisición de certificado de sitio seguro SSL para sitios web de la Contraloría de Bogotá D.C.	02/13/2026	$ 1.986.881	Mínima cuantía	12 días
Agencia Nacional de Hidrocarburos	ANH-001-MIN-2026	593. Adquirir los certificados SSL de los portales web de la ANH para el acceso seguro a la información.	2/12/2026	$ 3.970.286	Mínima cuantía	2 meses
Hospital Departamental Centenario ESE	006-2026	Compra de certificado SSL tipo Wildcard para reporte de rips según lo exigido resolución 0558 de 2024.	01/30/2026	$ 2.354.560	Contratación régimen especial	33 días
			PROMEDIO	**$ 3.008.547**		

Fuente: Plataforma SECOP II, consulta realizada en octubre de 2026, vigencia 2026.

Del análisis de los procesos de referencia consultados en la plataforma SECOP II para la vigencia 2026, se evidencia que los valores contratados presentan una dispersión significativa, lo cual es consistente con la variabilidad propia de las condiciones comerciales bajo las cuales los proveedores estructuran sus ofertas en los diferentes procesos de contratación pública.

Desde el punto de vista del análisis estadístico de precios, y con el fin de obtener un valor representativo del comportamiento del mercado, la Entidad realizó un ejercicio de depuración de la información, identificando y excluyendo aquellos valores que se consideran atípicos o extremos, con base en criterios de consistencia, concentración de datos y razonabilidad

técnica, en línea con las buenas prácticas de análisis de mercado aplicables a los estudios previos en contratación pública.

Este procedimiento permite evitar sesgos en la estimación derivados de valores que no reflejan el comportamiento central del mercado. En particular, se identificaron dos registros que fueron excluidos del análisis por las siguientes razones técnicas:

- **Verificación de instrumentos de agregación de demanda (Acuerdo Marco de Precios) Tienda Virtual del Estado Colombiano**

Previo a la elaboración del presente estudio, se verificó en la Tienda Virtual del Estado Colombiano, administrada por Colombia Compra Eficiente, la existencia de instrumentos de agregación de demanda aplicables a la adquisición del bien requerido.

Como resultado de esta revisión, se identificó que el Acuerdo Marco de Precios CCE-309-AMP-2022, denominado "Productos y Servicios Electrónicos y Digitales de Confianza", contempla dentro de su Lote 2 la adquisición de certificados digitales de sitio seguro SSL en sus modalidades DV, OV y EV, por lo que, en principio, podría atender la necesidad objeto de este proceso. Sin embargo, dicho Acuerdo Marco se encuentra cerrado para la generación de nuevas órdenes de compra desde el 27 de diciembre de 2025, permitiéndose únicamente la ejecución de aquellas emitidas con anterioridad a esa fecha y hasta el 27 de diciembre de 2026.

Igualmente, se verificó el Acuerdo Marco de Servicios de Conectividad IV, actualmente vigente, encontrándose que su catálogo no incluye certificados digitales de sitio seguro SSL/TLS. Aunque dentro de sus servicios contempla la opción denominada «VPN Client to Site SSL», esta corresponde a un servicio de conectividad remota que utiliza el protocolo SSL como mecanismo de cifrado para el establecimiento de túneles VPN y no a un servicio de certificación digital de dominios, por lo que no satisface la necesidad que se pretende contratar.

En consecuencia, a la fecha de elaboración del presente estudio no existe un Acuerdo Marco de Precios vigente y aplicable para la adquisición de los certificados digitales SSL/TLS requeridos por la Entidad. Por tal razón, la Contraloría Distrital de Medellín adelanta el correspondiente proceso de contratación mediante la modalidad de selección de Mínima Cuantía, conforme se desarrolla en el numeral 3 del presente estudio.

Sin embargo, se revisaron los valores publicados en el catálogo del Acuerdo Marco de Precios CCE-309-AMP-2022 con fecha del 07/04/2025, realizando el incremento del IPC con corte a la vigencia 2025 del 5,10% para el servicio de actualización de certificados digitales SSL/TLS, evidenciando una variabilidad significativa entre los diferentes proveedores, con valores que oscilan aproximadamente entre $604.128 y $16.417.511, con las características de OV - Subdominio SAN o OV – Wilcard, dejando un promedio cercano a $3.904.820.

Catálogo V3 – Lote 2

CODIGO	NOMBRE	Característica 1	Característica 2	Característica 3	Unidad de facturación	GSE SA ACT IPC 2025	Certicámara SA ACT IPC 2025	Camerfirma ACT IPC 2025	PROMEDIO
AMSEDC-SSL-02 -5	Certificado digital de sitio web SSL OV Validación Organización	Certificado SSL - OV - Subdominio SAN	2 años	Todas las Zonas	Certificado	$ 2.069.326	$ 3.552.343	$ 574.813	**$ 1.944.082**
AMSEDC-SSL-02 -6	Certificado digital de sitio web SSL OV Validación Organización	Certificado SSL - OV - Wilcard	2 años	Todas las Zonas	Certificado	$ 3.908.727	$ 15.672.227	$ 3.218.952	**$ 7.662.604**
					IPC 2025 5,10%	$ 2.174.862	$ 3.733.513	$ 604.128	**$ 2.043.231**
						$ 4.108.072	$ 16.471.511	$ 3.383.118	**$ 8.053.397**
								PROMEDIO	**$ 3.904.820**

Desde el punto de vista del análisis de precios, dicha variabilidad refleja la existencia de diferentes estructuras de costos, márgenes comerciales y condiciones de oferta de los proveedores, lo cual incide directamente en la formación del precio dentro del Acuerdo Marco.

En este contexto, los valores del catálogo se consideran como una referencia amplia del mercado, pero no como un indicador puntual del valor del servicio requerido, en la medida en que no reflejan el comportamiento central de los precios observados en procesos de contratación efectiva ni permiten identificar directamente valores representativos.

Por lo anterior, dichos valores son utilizados como elemento de contraste dentro del análisis de mercado, mas no como base para la determinación del presupuesto oficial.

- **Análisis histórico del mercado**

De igual manera, se analizaron valores históricos correspondientes a la vigencia 2025, incluyendo procesos de contratación publicados en la plataforma SECOP II con objeto contractual comparable, específicamente relacionados con la actualización de certificados digitales SSL/TL.

Procesos de referencia SECOP II -2025

Entidad	Referencia del Proceso	Descripción del Procedimiento	Fase Selección	Precio Base	Modalidad de Contratación	Duración
Unidad de Búsqueda de Personas Desaparecidas	UBPD-MC-031-2025	OTIC-576 Adquirir el Certificado digital SSL tipo Wildcard para el dominio de la página web y sus subdominios de la Unidad de Búsqueda de Personas Dadas por Desaparecidos en razón y en contexto del conflicto armado	12/05/2025	$ 4.222.000	Mínima cuantía	8 días
ESE Hospital Departamental Universitario del Quindío San Juan de Dios	CCV-0045-2025	Adquisición de un certificado SSL (tipo Wildcard OV) para el dominio www.hospitalquindio.gov.co de la E.S.E. Hospital Departamental Universitario del Quindío San Juan de Dios, para dar cumplimiento a la Resolución 2275 de 2023 del Ministerio de Salud.	11/25/2025	$ 3.349.600	Contratación régimen especial	5 días
E.S.E Hospital del Rosario	OC-0000000002 30 de 2025	Suministro de certificado de dominio SSL optimum Wildcard para la E.S.E. Hospital del Rosario.	11/01/2025	$ 1.606.500	Contratación régimen especial	17 días
Superintendencia de la Economía Solidaria	MC-14-2025	Contratar la adquisición del certificado digital SSL tipo Wildcard para la Supersolidaria.	10/21/2025	$ 3.600.000	Mínima cuantía	30 días
Financiera de Desarrollo Nacional S.A.	FDN-ADM-4402597-25	El objeto de la presente orden es la Adquisición de certificado de sitio seguro SSL/TLS, Tipo Geotrust True Business ID SSL OV Wildcard para el dominio *.fdn.com.co	10/10/2025	$ 3.110.955	Contratación régimen especial	6 días
UPME	DIRECTA 371-2025	Adquirir Certificado Wildcard SSL Multidominio para los servidores de la Unidad.	10/06/2025	$ 1.500.000	Contratación régimen especial	12 meses
Institución Universitaria de Barranquilla-IUB	MC-IUB-019-2025	Adquisición de un certificado SSL Wildcard con vigencia de un año, que garantice la seguridad, la autenticidad y confiabilidad en el acceso a la página web de la Institución Universitaria de Barranquilla, desde cualquier navegador de internet.	9/02/2025	$ 3.387.388	Mínima cuantía	1 mes
Contraloría Municipal Itagüí	CMI-MC01-2025	Adquisición del certificado SSL Wildcard para la Contraloría Municipal de Itagüí.	01/27/2025	$ 2.344.153	Mínima cuantía	2 días
Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas IPSE	IMC-001-2025	Adquisición de certificado TLS / SSL Wildcard con vigencia de 2 años para los sitios web del IPSE	01/24/2025	$ 3.714.312	Mínima cuantía	20 días

Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas IPSE	IMC-001-2025	Adquisición de certificado TLS / SSL Wildcard con vigencia de 2 años para los sitios w eb del IPSE	01/24/2025	$ 3.714.312	Mínima cuantía	20 días
Hospital Departamental Centenario ESE	002-2025	Compra certificado SSL tipo Wildcard para reporte de rips según lo exigido Resolución 0558 de 2024.	01/21/2025	$ 2.238.176	Contratación régimen especial	44 días
			PROMEDIO	**$ 2.980.672**		

Fuente: Plataforma SECOP II, consulta realizada en octubre de 2026, vigencia 2025.

El análisis de esta información histórica resulta relevante en la medida en que permite contar con un referente temporal que facilita la validación de los valores observados en la vigencia actual, así como la identificación de tendencias en la evolución del mercado.

En este sentido, al comparar los valores históricos con los obtenidos en la vigencia 2026, incluyendo los procesos de referencia en SECOP II, las cotizaciones recibidas y los resultados del Acuerdo Marco de Precios, se observa coherencia en los rangos de precios, así como una ligera tendencia al incremento en los valores más recientes.

Esta variación se considera consistente con la dinámica del mercado y no representa una ruptura estructural en la formación de precios del servicio, sino una evolución dentro de los rangos esperados.

En concordancia con lo anterior, el comportamiento histórico del mercado refuerza la validez del análisis de dispersión y depuración de datos realizados para la vigencia actual, confirmando que el valor estimado adoptado se encuentra alineado con el comportamiento central del mercado y no obedece a variaciones atípicas o coyunturales.

Análisis del mercado (cotizaciones)

En desarrollo del estudio de mercado, la Entidad realizó solicitud de cotización y consultas en internet de proveedores habilitados para prestar este tipo de servicio, como resultado de dichas solicitudes, se obtuvo lo siguiente:

Ítem	Descripción	Cant.	CAMERFIRMA	CERTICAMARA	SECTIGO	HOSTING	Promedio Mercado

1	Adquisición y actualización de un (1) certificado digital de sitio seguro tipo Secure Site Ov (SSL-Ov), en modalidad Wildcard con dominios adicionales (SAN), para los dominios y subdominios institucionales de la Contraloría Distrital de Medellín. Por 2 años.	1	$2.570.000	$6.130.963	$2.551.200	$2.960.000	**$3.553.041**
Fuente datos:			**COTIZACIÓN 2052-9092026 09/08/2026**	**COTIZACIÓN #009794 23/09/2026**	Certificados SSL Wildcard OV | Sectigo® Oficial CONSULTADA EL 09/10/2026	https://checkout.hosting.com/order/basket/	

Lo anterior evidencia que los valores obtenidos en el mercado abierto son consistentes con los procesos de referencia en SECOP II y con la simulación realizada mediante el Acuerdo Marco de Precios.

Análisis comparativo de fuentes de precio y sustentación del valor estimado

Para la estructuración del presupuesto oficial, la Entidad consideró de manera integral las distintas fuentes de información de mercado disponibles, a saber: los procesos de referencia identificados en la plataforma SECOP II para la vigencia 2026, las cotizaciones recibidas de proveedores del sector y la simulación realizada mediante el Simulador AMP del Acuerdo Marco de Precios CCE-309-AMP-2022.

Respecto a las cotizaciones recibidas, se obtuvieron dos: CERTICAMARA por valor de $6.130.963 y CAMERFIRMA por valor de $$2.570.000. Se agregan dos consultas realizadas en las páginas oficiales de SECTIGO por $2.551.200 y de HOSTING por $2.960.000; arrojando un promedio de $3.553.041. Si bien las dos cotizaciones recibidas constituyen una fuente válida de referencia comercial, presentan un margen que se aleja del análisis de la contratación promedio revisada en SECOP II 2026 de $3.008.547.

En este contexto, y dado que tanto el promedio de cotizaciones como la simulación AMP ($3.904.820) se ubican por encima del rango de concentración del mercado identificado en SECOP II 2026, la Entidad considera técnicamente más sólido y prudente adoptar como presupuesto oficial el valor resultante del análisis depurado de los procesos de referencia en SECOP II, fuente que refleja con mayor fidelidad el comportamiento real y efectivo del mercado para este tipo de servicio en la vigencia analizada.

De esta manera, el valor adoptado no corresponde a una única fuente de información, sino a la integración técnica de las diferentes fuentes analizadas, priorizando aquellas que reflejan el comportamiento efectivo del mercado.

En consecuencia, se confirma el presupuesto oficial estimado de TRES MILLONES OCHO MIL QUINIENTOS CUARENTA Y SIETE PESOS M/CTE ($3.008.547), valor alineado con el rango central del mercado, que garantiza condiciones de competencia efectiva en el proceso y reduce el riesgo de una declaratoria de desierta que pudiera comprometer la continuidad del servicio dentro de los plazos requeridos.

Valor estimado: $3.008.547.

Se establece como valor estimado del contrato para la presente vigencia la suma de **TRES MILLONES OCHO MIL QUINIENTOS CUARENTA Y SIETE PESOS M/CTE ($3.008.547)**, valor que se adopta como una estimación técnicamente robusta, representativa y consistente con el comportamiento central del mercado, conforme al análisis integral de las fuentes de información realizado por la Entidad.

Este valor incluye el Impuesto al Valor Agregado (IVA), todos los costos directos e indirectos, así como los impuestos, tasas y contribuciones a que haya lugar, necesarios para la ejecución integral del objeto contractual.

Forma de pago:

La Contraloría Distrital de Medellín pagará el valor total del contrato en un (1) solo pago, dentro de los treinta (30) días calendario siguiente a la radicación del acta de recibo a satisfacción suscrita por el supervisor del contrato.

El precio pactado es global e indivisible y corresponde a la adquisición de un (1) certificado digital SSL Wildcard con validación de organización (OV), con una vigencia de dos (2) años, contados a partir de su emisión. El valor incluye las renovaciones que se requieran durante la vigencia del certificado, sin que estas generen costos adicionales para la entidad, de conformidad con las condiciones técnicas y comerciales establecidas para el proceso.

El pago se efectuará una vez se haya realizado la emisión, instalación y puesta en funcionamiento del certificado, previa verificación del cumplimiento de las especificaciones técnicas y recibo a satisfacción por parte de la supervisión del contrato, así como de los demás requisitos administrativos y legales exigidos para el pago.

Cada pago se realiza dentro de los treinta (30) días calendario siguiente a la radicación del acta de recibo a satisfacción suscrita por el supervisor del contrato

El contratista deberá enviar la factura o cuenta de cobro con todos sus anexos a través de la plataforma SECOP II (formulario 7), del 1 al 20 de cada mes; la cual será verificada y aprobada por el supervisor del contrato.

Anexos:

- Informe escrito de actividades realizadas, acompañado de las respectivas evidencias, suscrito por el contratista. Este informe debe detallar claramente las actividades desarrolladas según las obligaciones específicas del contrato y acorde a las actividades planificadas en cada periodo.
- Factura electrónica debidamente diligenciada con todos los ítems debidamente detallados, según lo acordado en la oferta económica (deberá ser enviada al correo recepcionfacturas@cdm.gov.co del 1 al 20 de cada mes).
- Cuenta de Cobro debidamente diligenciada, cuando no le aplique la factura electrónica.
- Planilla comprobante de pago de seguridad social por el respectivo periodo que se está causando, en la forma y cuantía como lo ordenan las normas en esta materia (para persona natural).
- Para persona jurídica: debe adjuntar la constancia de que se encuentra al día con el pago de aportes por los últimos seis (6) meses, al sistema de seguridad social integral, así como de los aportes a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje SENA, cuando corresponda. Si este certificado es expedido por el Revisor Fiscal, se debe anexar certificado de la Junta Central de Contadores vigente, en el que se indique que no tiene sanciones disciplinarias y así mismo la tarjeta profesional.

Concordancia del objeto del contrato con el rubro presupuestal:

Para el logro de los objetivos previstos y el servicio a contratar acorde con el objeto y sus especificaciones técnicas, descrito en este estudio previo, el valor estimado del presupuesto oficial que se destinará para el proceso contractual será de: **TRES MILLONES OCHO MIL QUINIENTOS CUARENTA Y SIETE PESOS M/CTE ($3.008.547)**, incluidos los impuestos, tasas y contribuciones que por ley correspondan, con cargo al rubro presupuestal No. **212020100400** denominado **"Otros productos metálicos y paquetes de software**" de acuerdo con el Plan Anual de Adquisiciones 2026. Según Certificado de Disponibilidad Presupuestal **Nro. 1013319** del 04 de noviembre del 2026, expedido por la Dirección

Administrativa de Recursos Físicos y Financieros de la Entidad. Documento que hará parte integral de este estudio previo.

ESTAMPILLA PARA LA JUSTICIA FAMILIAR: corren a cargo del CONTRATISTA los impuestos, tasas y/o retenciones de Ley o los que determinen los respectivos acuerdos del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, que surjan de este contrato**.** La Contraloría Distrital de Medellín de conformidad con el artículo 22 y siguientes de la Ley 2126 del 2021 y el artículo 307 y siguientes del Acuerdo Municipal #93 del 2023; tiene a cargo la aplicación de la Estampilla para la Justicia Familiar, equivalente al dos por ciento (2%) del valor del pago anticipado si lo hubiere, y de cada cuenta que se le pague al contratista. La base gravable es el valor bruto de los contratos, entendido como el valor a girar por cada orden de pago o anticipo sin incluir el impuesto al valor agregado IVA.

Exclusión: están excluidos del pago de la Estampilla para la Justicia Familiar los contratos de prestación de servicios inferiores a 10 SMLMV mensuales.

La Contraloría Distrital de Medellín efectuará las retenciones que en materia tributaria tenga establecida la Ley y respecto de las cuales sea su obligación efectuar la retención. En los demás casos, el contratista deberá cumplir con el pago de los impuestos, tasas o contribuciones que se deriven de la presente contratación, si es del caso.

5. LOS CRITERIOS PARA SELECCIÓNAR LA OFERTA MAS FAVORABLE:

De conformidad con lo dispuesto en el numeral 5 del artículo 2 de la Ley 1150 de 2007, modificado por el artículo 94 de la Ley 1474 de 2011, y en la Subsección 5 de la Sección 1 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, para los procesos adelantados bajo la modalidad de selección de mínima cuantía la Entidad seleccionará la oferta más favorable teniendo en consideración el cumplimiento de los requisitos habilitantes exigidos y el menor precio ofertado.

En consecuencia, la Contraloría Distrital de Medellín evaluará las ofertas presentadas verificando, en primer lugar, el cumplimiento de los requisitos habilitantes de carácter jurídico exigidos en la invitación pública y, posteriormente, el cumplimiento de las condiciones técnicas mínimas establecidas para la ejecución del objeto contractual.

La Entidad verificará que el oferente cuente con capacidad jurídica para contratar, no se encuentre incurso en causales de inhabilidad, incompatibilidad o conflicto de interés, acredite

el cumplimiento de sus obligaciones frente al Sistema de Seguridad Social Integral y aportes parafiscales cuando haya lugar, y cumpla los demás requisitos habilitantes definidos en la invitación pública.

Igualmente, se verificará que la propuesta atienda integralmente las especificaciones técnicas mínimas requeridas por la Entidad para la adquisición y actualización de los certificados digitales SSL/TLS, de conformidad con las condiciones, características, alcances y requerimientos establecidos en los documentos del proceso.

Una vez efectuada la verificación de los requisitos habilitantes y del cumplimiento de las especificaciones técnicas exigidas, la Contraloría Distrital de Medellín procederá a determinar el orden de elegibilidad con fundamento en el menor valor económico ofertado, seleccionando la propuesta que represente la oferta más favorable para la Entidad bajo criterios de economía, eficiencia y selección objetiva.

La oferta más favorable será aquella que:

a) Cumpla la totalidad de los requisitos habilitantes establecidos en la invitación pública.
b) Cumpla integralmente las especificaciones y condiciones técnicas mínimas exigidas por la Entidad.
c) No presente causales de rechazo previstas en la invitación pública.
d) Presente el menor precio total ofertado para la ejecución del objeto contractual.

La verificación de los requisitos habilitantes no otorgará puntaje alguno y tendrá como único propósito determinar si el oferente se encuentra habilitado para ejecutar el objeto contractual, conforme a lo previsto en la normativa vigente de contratación estatal.

En caso de presentarse empate entre dos o más ofertas que cumplan la totalidad de los requisitos habilitantes y de las condiciones técnicas exigidas, así como el mismo valor económico ofertado, la Entidad aplicará los criterios de desempate establecidos en el artículo 35 de la Ley 2069 de 2020 y las disposiciones reglamentarias contenidas en el Decreto 1082 de 2015, privilegiando, en el orden legalmente previsto, aquellos proponentes que acrediten las condiciones definidas por el legislador como medidas de promoción empresarial y

fortalecimiento de la participación de población en condición de vulnerabilidad, garantizando en todo caso los principios de transparencia, igualdad, selección objetiva y libre concurrencia. Por consiguiente, la selección del contratista recaerá en el proponente que, además de satisfacer integralmente las exigencias jurídicas y técnicas definidas por la Contraloría Distrital de Medellín, presente la oferta económica de menor valor, de conformidad con las reglas previstas para los procesos de mínima cuantía.

6. ANÁLISIS DE RIESGO Y LA FORMA DE MITIGARLO:

El riesgo es un evento que puede generar efectos adversos y de distinta magnitud en el logro de los objetivos del Proceso de Contratación o en la ejecución del contrato. Siguiendo los parámetros establecidos por Colombia Compra Eficiente, se procede a continuación a la identificación, clasificación, tipificación, valoración y asignación de los **riesgos previsibles** que se puedan ocasionar desde la planeación del contrato, hasta su ejecución, así como la forma de mitigarlos y probabilidades de ocurrencia:

Riesgos Previsibles: Son los posibles hechos o circunstancias que por la naturaleza del proceso, la actividad a ejecutar o por la experiencia de la Entidad, es factible su ocurrencia.

Tabla para la valoración de la probabilidad y del impacto del riesgo:

PROBABILIDAD/IMPACTO	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
RARO (1)	2	3	4	5	6
IMPROBABLE (2)	3	4	5	6	7
POSIBLE (3)	4	5	6	7	8
PROBABLE (4)	5	6	7	8	9
CASI CIERTO (5)	6	7	8	9	10

Probabilidad del riesgo: **1) Raro** (puede ocurrir excepcionalmente); **2) Improbable** (puede ocurrir ocasionalmente);**3) Posible** (puede ocurrir en cualquier momento futuro); **4) Probable** (probablemente va a ocurrir); **5) Casi cierto** (ocurre en la mayoría de las circunstancias).

Impacto: afecta la ejecución del contrato o genera sobrecostos, así: **1) Insignificante:** no es trascendente; **2) Menor:** dificulta o genera sobrecostos de manera baja; **3) Moderado:** afecta la ejecución del contrato sin alterar el beneficio para las partes o afecta levemente el valor del contrato; **4) Mayor:** obstruye la ejecución del contrato sustancialmente, pero permite la consecución del objeto contractual o afecta notoriamente el valor del contrato; **5) Catastrófico:** perturba la ejecución del contrato de manera grave, imposibilitando la ejecución del objeto del contrato o afecta altamente el valor del contrato.

N	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le asigna?	Tratamiento/ Control a ser implementado	Impacto después del tratamiento				¿Afecta la ejecución del contrato?	Responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza el monitoreo?	Periodicidad
1	Específico	Externo	Ejecución	Operacional	Vencimiento del certificado sin renovar oportunamente, por la reducción progresiva de la vigencia máxima (CA/Browser Forum).	1. Indisponibilidad del sitio web y sistemas de información institucionales. 2. Advertencias de seguridad para los ciudadanos y funcionarios que accedan a los servicios. 3. Pérdida de imagen institucional. 4. Posible incumplimiento de las políticas de Gobierno Digital y seguridad de la información.	3	4	12	Alto	CDM-Contratista	Se mitiga exigiendo al contratista el método de validación de dominio (DCV) por CNAME con delegación persistente, que permite automatizar las reemisiones, y estableciendo alertas automáticas de vencimiento (30, 15 y 5 días antes) a cargo del proveedor.	1	2	2	Bajo	Sí	Supervisión-Contratista	Desde la suscripción del acta de inicio	Finalización de la ejecución del contrato	Seguimiento de las alertas de vencimiento y verificación periódica de la vigencia del certificado instalado.	Permanente
2	General	Externa	Ejecución	Económico	Variación de precios	Son los efectos derivados del incremento en el costo de los certificados digitales SSL en el mercado durante la ejecución del contrato, que podría generar un desequilibrio económico del contrato.	3	3	9	Alto	Contratista	Este riesgo lo asume el contratista, realizando una estimación adecuada de los costos, procesos y riesgos.	2	2	4	Moderado	Sí	Supervisión-Contratista	Desde la apertura del proceso de contratación	Finalización de la ejecución del contrato	En cada informe de supervisión.	Mensual o por pago único

3	Específico	Interna	Ejecución	Operacional	Modificación de especificaciones técnicas	Ocurre cuando el contratista hace entrega del certificado sin el cumplimiento de las especificaciones técnicas mínimas establecidas en los estudios previos	3	3	9	Alto	CDM-Contratista	Este riesgo lo asume la CDM, como beneficiaria final del servicio, siempre que no afecte el equilibrio económico del contrato de manera desproporcionada; se mitiga con la verificación técnica del certificado emitido frente a lo exigido en el numeral 2.	2	2	4	Moderado	Sí	Supervisión	Una vez se informe por parte de la Supervisión	15 días después	En cada informe de supervisión.	Mensual o por pago único
4	Específico	Externo	Ejecución contractual / etapa posterior a la ejecución	Operacional	Incumplimiento, omisión o demora por parte del proveedor en la gestión de las renovaciones de los certificados SSL Wildcard OV durante el periodo de cobertura contratado, debido a la dependencia de la entidad respecto del proveedor para mantener la continuidad de la certificación digital.	1. Vencimiento de los certificados SSL. 2. Alertas de seguridad en los navegadores. 3. Pérdida de confianza de los usuarios. 4. Interrupción o afectación del acceso a los sistemas y servicios web institucionales. 5. Exposición a riesgos de suplantación o interceptación de comunicaciones.	3	4	12	Alto	Proveedor / Contratista	Establecer contractualmente la obligación del contratista para que durante veinticinco (25) meses garantice la disponibilidad de las reemisiones o nuevas emisiones sucesivas exigidas por las reglas de la autoridad certificadora y del CA/Browser Forum, así como su instalación, configuración y soporte de garantizar la vigencia de los certificados durante el periodo contratado y efectuar las renovaciones que correspondan, sin costos adicionales cuando así se haya pactado. Exigir	2	2	4	Moderado	Sí	Supervisión-Contratista	Desde la suscripción del acta de inicio.	Al finalizar el periodo de las obligaciones de reemisión, instalación, configuración y soporte de los certificados, según las obligaciones contractuales.	Seguimiento al calendario de vencimientos, revisión periódica de la vigencia de los certificados instalados, verificación de las notificaciones del proveedor y comprobación de las renovaciones efectuadas.	Mensual y con alertas adicionales previas al vencimiento.

												notificación anticipada de vencimientos, confirmación de cada renovación, entrega de los certificados actualizados y acompañamiento técnico para su instalación. Este riesgo se mitiga con la constitución de la garantía única de cumplimiento con vigencia que ampare todo el período durante el cual subsisten las obligaciones de reemisión, instalación, configuración y soporte										

7. LAS GARANTÍAS QUE LA ENTIDAD ESTATAL CONTEMPLA EXIGIR EN EL PROCESO DE CONTRATACIÓN:

Si bien el plazo de ejecución del contrato corresponde a diez (10) días calendario, dicho término comprende únicamente las actividades iniciales de emisión, validación, entrega, instalación y puesta en funcionamiento del certificado digital SSL/TLS requerido por la Entidad. No obstante, el objeto contractual incorpora obligaciones que subsisten durante un período de cobertura comercial de veinticuatro (24) meses, relacionadas con las actualizaciones del certificado, su instalación, configuración, soporte técnico especializado y demás actividades necesarias para garantizar la continuidad y disponibilidad del servicio contratado.

La exigencia y vigencia de la garantía se sustenta en el análisis y asignación de riesgos efectuado por la Entidad. En particular, la matriz de riesgos identificó el **Riesgo No. 4**, consistente en el incumplimiento, omisión o demora por parte del proveedor en la gestión de las renovaciones, actualizaciones, instalación, configuración y soporte de los certificados SSL durante el período de cobertura contratado. Dicho riesgo fue asignado al contratista y su

materialización puede ocurrir durante todo el período de cobertura comercial (incluyendo el periodo posterior a la entrega inicial del certificado). Asimismo, dentro de las medidas de tratamiento establecidas para este riesgo se dispuso expresamente la constitución de una garantía que ampare la totalidad del período durante el cual subsisten dichas obligaciones.

Lo anterior obedece a las reglas adoptadas por el CA/Browser Forum y las autoridades certificadoras internacionales, las cuales han reducido progresivamente la vigencia máxima de los certificados SSL/TLS, circunstancia que exige la realización de actualizaciones sucesivas durante el tiempo de cobertura contratado. En consecuencia, las obligaciones del contratista no se agotan con la emisión inicial del certificado, sino que se extienden durante todo el período de cobertura adquirido.

De conformidad con los principios de responsabilidad, protección del patrimonio público y adecuada administración de los riesgos contractuales previstos en la Ley 80 de 1993 y en los artículos 2.2.1.2.3.1.1 y siguientes del Decreto 1082 de 2015, la Entidad considera necesario que el amparo de cumplimiento cubra la totalidad del período durante el cual permanece asignado al contratista el Riesgo No. 4 de la matriz de riesgos, garantizando la efectividad de los mecanismos de protección frente a eventuales incumplimientos relacionados con las obligaciones de actualización, renovación, instalación, configuración y soporte técnico.

Amparo de cumplimiento: el contratista deberá constituir una garantía de cumplimiento por una cuantía equivalente al diez por ciento (10%) del valor del contrato, con una vigencia de veinticuatro (24) meses contados a partir de la fecha de inicio registrada en SECOP II. Dicha vigencia comprende el plazo de ejecución contractual de diez (10) días y el período de cobertura comercial de veinticuatro (24) meses durante el cual subsisten las obligaciones de actualización, instalación, configuración, soporte técnico y continuidad del servicio.

8. LA INDICACIÓN DE SI EL PROCESO DE CONTRATACIÓN ESTA COBIJADO POR UN ACUERDO COMERCIAL:

De conformidad con lo establecido en el Manual para el manejo de los Acuerdos Comerciales en Procesos de Contratación expedido por Colombia Compra Eficiente, las Entidades Estatales sometidas al Estatuto General de Contratación Pública deben verificar en la etapa de planeación la aplicabilidad de los Acuerdos Comerciales a cada proceso de contratación. No obstante, el citado Manual precisa que las Entidades Estatales que adelantan procesos de contratación bajo la modalidad de mínima cuantía no están obligadas a efectuar dicho análisis.

En consideración a que el presente proceso se adelantará mediante la modalidad de Selección de Mínima Cuantía, la Contraloría Distrital de Medellín concluye que no resulta procedente efectuar el análisis de cobertura de los Acuerdos Comerciales vigentes, razón por la cual las obligaciones derivadas de dichos instrumentos internacionales en materia de compras públicas no son aplicables al presente proceso de selección.

9. LOS DEMÁS ASPECTOS DERIVADOS DE LA COMPLEJIDAD DEL OBJ CONTRACTUAL QUE SOPORTEN LOS REQUERIMIENTOS QUE SE INCLUYEN EN DOCUMENTOS ANEXOS DEL PROCESO

9.1. MULTAS:

En caso de mora, incumplimiento parcial u omisión injustificada de las obligaciones adquiridas por el contratista y sin perjuicio de la declaratoria de caducidad, la Contraloría Distrital de Medellín, mediante resolución motivada podrá imponer multas cuyo valor se liquidará con base en un uno por ciento (1%) sobre el valor total del contrato por cada día de retraso hasta por un plazo de diez (10) días calendario.

En los siguientes casos las multas serán: **1.** En caso de mora o incumplimiento parcial de las obligaciones que adquirirá el contratista sin perjuicio de la declaratoria de caducidad del contrato, la Entidad podrá mediante resolución motivada imponer multas diarias por cada día de mora, equivalentes hasta el 0.3% del valor total del contrato. **2.** En caso de incumplimiento del término para legalizar en forma debida el contrato, el cual es de cinco (5) días hábiles a partir de su firma, se impondrá una multa del (0.1%) del valor del contrato por cada día de atraso injustificado. **3.** Por incumplimiento de la obligación de iniciar la ejecución del contrato de acuerdo con la fecha de inicio en la plataforma SECOP II, 0.1% del valor del contrato por cada día de atraso injustificado. **4.** Por incumplimiento en el plazo inicialmente acordado en el contrato, el 0.2% del valor del contrato por cada día de atraso injustificado. Lo anterior sin perjuicio de la declaratoria de incumplimiento parcial del contrato.
En ningún caso la sumatoria de las multas impuestas deberá ascender a una suma mayor al diez por ciento (10%), del valor del contrato.

Una vez declarado el incumplimiento del contrato por parte de la Contraloría, el valor de las multas se tomará directamente de cualquier suma que se le adeude al contratista, sin perjuicio de hacer efectiva la cláusula penal o la Garantía de Cumplimiento del contrato, y si esto no fuere posible, se procederá al cobro coactivo de conformidad con lo previsto en el artículo 17 de la Ley 1150 de 2007.

La imposición de multas, así como su pago o deducción, no exoneran al contratista del cumplimiento de sus obligaciones contractuales, so pena de que se le inicie un nuevo procedimiento sancionatorio ante nuevos incumplimientos.

9.2 CLÁUSULA PENAL

En caso de incumplimiento grave por parte del contratista de las obligaciones a su cargo, la Contraloría cobrará a título de pena, una sanción pecuniaria equivalente al diez por ciento (10%) del valor total del contrato, que se tendrá como pago parcial de los perjuicios que se le ocasionen a la Entidad, quien podrá descontar la sanción de cualquier suma que se le adeude al contratista si la hubiere, o de la Garantía de Cumplimiento constituida, y si esto no fuera posible, se procederá al cobro coactivo de conformidad con lo previsto en el artículo 17 de la Ley 1150 de 2007 en concordancia con el 86 de la Ley 1474 de 2011.

El valor de la cláusula penal que se haga efectivo se considerará como pago parcial, pero no definitivo de los perjuicios ocasionados a la Entidad, quien podrá reclamar los perjuicios que excedan del monto de la cláusula penal.

La aplicación de la cláusula penal podrá hacerse efectiva en los eventos señalados, sin perjuicio del cumplimiento de la obligación principal por parte del contratista.

10. OBLIGACIONES DEL CONTRATISTA Y LA CONTRALORÍA DISTRITAL DE MEDELLÍN:

10.1. Obligaciones Generales del contratista:

- Ejecutar el objeto del contrato, y las obligaciones contractuales de manera eficaz y oportuna, en las condiciones de tiempo, modo, lugar, cantidad, cobertura, calidad y con las especificaciones establecidas por la Contraloría para esta contratación.
- Atender los requerimientos que le sean efectuados por el Supervisor del contrato y/o por la Contraloría, en los términos y las condiciones pertinentes.
- Registrar en el aplicativo SIGEP II, la hoja de vida, de conformidad con lo establecido en el Decreto 1083 de 2015 Art. 2.2.17.10, para la correcta ejecución del contrato (cuando aplique).
- Asumir el pago de los impuestos, gravámenes, de cualquier género que establezcan las leyes colombianas y demás erogaciones necesarias para la ejecución del contrato.
- Asumir el pago de las obligaciones laborales correspondientes a los trabajadores vinculados a la ejecución del contrato

- Conocer y aplicar la normativa vigente y los lineamientos internos de la Entidad en el desarrollo de las funciones contractuales y para el cumplimiento de las demás actividades que le sean asignadas.
- Rendir los informes que sean requeridos por la supervisión del contrato.
- Atender y acatar las recomendaciones y sugerencias que le sean formuladas por el Supervisor del contrato.
- Hacerse cargo del equipo humano de trabajo que sea necesario, el suministro de insumos y la logística requerida.
- Conocer a cabalidad el estudio previo, la propuesta y el contrato, para realizar su ejecución con eficiencia y eficacia.
- Presentar previo a la firma e inicio en la plataforma SECOP II, los documentos necesarios para la ejecución del contrato.
- Suscribir conjuntamente con el supervisor los documentos que se requieran durante el desarrollo del contrato, y con el ordenador del gasto y supervisor el acta de liquidación si es el caso.
- Obligación sobre Seguridad Informática: El Contratista con la firma del presente contrato, se obliga a dar cumplimiento a las políticas y normas de seguridad informática de la Contraloría Distrital de Medellín, incorporadas en el Sistema de Integral Gestión, al cual podrá acceder, a través del Portal web de la Entidad www.cgm.gov.co por la opción Información Corporativa-Sistemas de Información-Isolución y allí aparecen las credenciales de acceso: **Usuario: consultasg, Clave: CDM12345**, una vez haya ingresado, dar clic en la opción documentación, opciones manuales donde encontrará el Manual Políticas de Operación de la Entidad (numeral Política Suministro de Bienes y Servicios). La trasgresión a los reglamentos o directrices, dará lugar a la aplicación de las sanciones correspondientes, sin perjuicio de la responsabilidad civil, penal o disciplinaria que recaiga sobre el Contratista.
- Cumplir con los trámites que como proveedor le asisten, en la plataforma SECOP II, entre los cuales se pueden enunciar la creación de usuario, carga de documentos del contrato, gestión de pagos y los demás solicitados por la Entidad.
- Las demás obligaciones que de acuerdo con su naturaleza se requieran para el cumplimiento del objeto del contrato.
- El proveedor se compromete a cumplir con la Política Antisoborno y la Política de regalos, hospitalidad, donaciones y beneficios que se encuentra publicada en la página web de la Contraloría Distrital de Medellín en el siguiente link:https://www.cdm.gov.co/cgm/Paginaweb/TAIP/Paginas/Pol%C3%ADtica-Antisoborno.aspx y Link:https://www.cdm.gov.co/cgm/Paginaweb/TAIP/Paginas/Pol%C3%ADtica-que-Regula-la-Oferta,-Suministro-o-Aceptaci%C3%B3n-de-Regalos.aspx

10.2. Obligaciones Específicas del contratista:

- Suministrar un (1) certificado digital SSL/TLS con validación de organización (OV), modalidad Wildcard, para el dominio *.cdm.gov.co, incluyendo los nombres alternativos cdm.gov.co y www.cdm.gov.co, con algoritmo de clave pública RSA de mínimo 2048 bits y algoritmo de firma SHA-256, conforme a las especificaciones técnicas establecidas en el estudio previo.
- Gestionar ante la autoridad de certificación (CA) los procesos de validación de la organización y del dominio, mediante el método de validación acordado con la Entidad. El certificado inicial deberá emitirse dentro de los cinco (5) días hábiles siguientes a la radicación completa de la documentación y los requisitos técnicos necesarios.
- Utilizar la solicitud de firma de certificado (CSR) generada por la Contraloría Distrital de Medellín, garantizando que la clave privada permanezca bajo la custodia exclusiva de la Entidad, sin solicitarla, acceder a ella ni conservarla.
- Entregar el certificado digital y su cadena de certificación correspondiente, incluyendo los certificados intermedios necesarios, en los formatos compatibles con las plataformas institucionales, junto con la documentación que permita verificar el nombre del dominio, los nombres alternativos, el tipo de validación y las fechas de vigencia.
- Realizar la instalación, configuración y verificación inicial del certificado en los servidores y servicios institucionales definidos por la Dirección de Desarrollo Tecnológico, previa coordinación con esta dependencia. La instalación deberá incluir la comprobación de la cadena de confianza y el funcionamiento correcto de las conexiones HTTPS.
- Garantizar, durante un periodo comercial contratado de veinticuatro (24) meses, la disponibilidad de las actualizaciones o nuevas emisiones sucesivas del certificado que sean necesarias para mantener la cobertura contratada, de conformidad con los requisitos vigentes de la autoridad de certificación y del CA/Browser Forum. Estas emisiones sucesivas deberán estar incluidas en el precio contractual, sin costos adicionales para la Entidad, y deberán efectuarse con la anticipación necesaria para evitar interrupciones en los servicios institucionales.
- Realizar la instalación y configuración de las nuevas emisiones del certificado que sean necesarias durante el periodo contratado, en coordinación con la Dirección de Desarrollo Tecnológico, y verificar que los servicios institucionales continúen operando correctamente bajo HTTPS.
- Remitir notificaciones de vencimiento próximo a los correos institucionales designados por la Entidad, con treinta (30), quince (15) y cinco (5) días calendario de anticipación a la fecha de vencimiento de cada certificado emitido, siempre que los mecanismos de

notificación de la CA lo permitan. Cuando el periodo de vigencia del certificado sea inferior a treinta días, las notificaciones deberán ajustarse para garantizar que se reciban oportunamente.

- Atender las solicitudes de soporte técnico relacionadas con la emisión, instalación, renovación o actualización del certificado dentro de un (1) día hábil siguiente a su radicación. El soporte requerido para mantener la cobertura contratada deberá estar incluido en el precio, sin perjuicio de los servicios adicionales que se pacten expresamente.
- Acreditar que el certificado será emitido por una autoridad de certificación reconocida por los principales navegadores y sistemas operativos, y aportar la documentación que permita verificar la confiabilidad de la cadena de certificación y las condiciones de respaldo o garantía del producto, cuando aplique.
- Gestionar, sin costo adicional, la revocación y nueva emisión del certificado cuando la Entidad lo solicite por motivos de seguridad, incluyendo la sospecha o el compromiso de la clave privada. Asimismo, informar oportunamente cualquier circunstancia que pueda afectar la confianza, validez o aceptación del certificado por parte de los navegadores y sistemas operativos.
- Entregar a la supervisión del contrato los soportes de emisión, instalación y configuración del certificado inicial, así como los documentos que acrediten las emisiones sucesivas realizadas durante el periodo de cobertura contratado, para efectos de seguimiento y verificación de las obligaciones.

10.3. Obligaciones del Contratista relativas al Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST):

De conformidad con las normas legales que regulan esta materia, y en el caso que se requiera que el contratista desplace personal a la sede de la Contraloría, la persona que se contrate, se obligará de conformidad con el contrato a:

- Disponer de canales de comunicación adecuados para los controles e inquietudes durante el desarrollo del contrato.
- Pagar por su propia cuenta y en forma puntual los pagos correspondientes a la Seguridad Social Integral (Salud, Pensiones y Riesgos Laborales), los parafiscales si está obligada por Ley a cumplir con dicha obligación y remitir oportunamente el comprobante de pago de seguridad social integral.

- Cuando sea solicitado participar en las actividades del Plan de Emergencias de la Contraloría Distrital de Medellín y de ser requerido asistir a las capacitaciones convocadas a través del Supervisor del Contrato.
- Reportar de manera oportuna las condiciones inseguras detectadas en el lugar de trabajo, es decir, en el sitio de la Contraloría donde preste físicamente el servicio.
- Reportar de manera oportuna los incidentes y accidentes de trabajo ocurridos en las instalaciones de la Contraloría.
- Para el ejercicio de las actividades, el contratista debe portar sus elementos de Bioseguridad y EPP asignados por sus jefes y requeridos para sus funciones.
- Presentar el soporte de la publicación realizada de estándares mínimos en la plataforma que dispuso el Ministerio de Trabajo en la página www.fondoderiesgoslaborales.gov.co, conforme al artículo 26 de la Resolución No. 0312 de 2019, que establece que, «Desde enero del año 2020 en adelante, (…) en el mes de diciembre las empresas deberán: 1. Aplicar la autoevaluación conforme a la Tabla de Valores y Calificación de los Estándares Mínimos del Sistema de Gestión de SST, mediante el diligenciamiento del formulario de evaluación establecido en el artículo 27 de dicha Resolución», y según la circular vigente expedida por el Ministerio del Trabajo.

10.4. Obligaciones de la Contraloría Distrital de Medellín:

- Ejercer la supervisión y control del cumplimiento del objeto y las obligaciones del presente contrato.
- Aprobar las garantías exigidas y que en debida forma se constituya a favor de la entidad.
- Facilitar todos los medios necesarios para el buen desarrollo del contrato.
- Pagar al CONTRATISTA la suma estipulada.
- Poner en conocimiento del CONTRATISTA la información que coadyuve o afecte la ejecución del contrato.
- Recibir a través de la supervisión del contrato los informes y demás documentos que se produzcan durante la ejecución del contrato.
- Suscribir con EL CONTRATISTA los documentos y las actas que correspondan.
- Suministrar al CONTRATISTA la información necesaria para llevar a cabo el objeto del contrato.
- Cumplir con los trámites que le asisten, en la plataforma SECOP II.

- Las demás que se deriven de la naturaleza del presente contrato y que surjan del desarrollo del mismo.
- Cumplir con lo establecido en la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Verificar que la hoja de vida del contratista se encuentre actualizada en SIGEP II, de acuerdo con el procedimiento y requisitos establecidos por el Decreto 1083 de 2015 Art. 2.2.17.10. Asimismo, vincular al contratista en SIGEP II durante la vigencia del contrato y desvincularlo cuando finalice el término contractual, con el fin de evidenciar la correcta gestión y trámite.

10.5. Obligaciones relativas al sistema de gestión de seguridad y salud en el trabajo (SG-SST) de la CDM:

- Procurar canales de comunicación para la gestión de seguridad y salud en el trabajo con el contratista.
- Verificar antes del inicio y durante la ejecución del contrato el cumplimiento de la obligación de afiliación al sistema general de riesgos laborales.
- Informar al contratista sobre las responsabilidades y compromisos con el SG-SST de la Contraloría Distrital de Medellín.
- Verificar durante el desarrollo de las actividades objeto del contrato el cumplimiento de la normativa en Seguridad y Salud en el trabajo.

11. CONFORMACIÓN EQUIPO DE TRABAJO Y EQUIPO DE PROCESO

El equipo de trabajo será conformado por el jefe de la dependencia y un equipo interdisciplinario (técnico, administrativo, económico y contable, su número de integrantes depende de la especialidad y complejidad del objeto contractual), designado por él, quién a su vez podrá demandar de personal de apoyo en cualquiera de las disciplinas académicas que preste sus servicios en otra dependencia de la Entidad a través del Ordenador del gasto. Deberá indicarse nombres y cargos de los integrantes, incluyendo el abogado que acompaña el proceso.

Nombre del servidor público	Cargo	Rol
Diego Mauricio Echeverri Arango	Director Administrativo de Desarrollo Tecnológico	Técnico, Económico, Contable y administrativo
Juan Pablo Sánchez Tirado	Técnico Operativo	Técnico y administrativo

Miguel ángel Ciro Orrego y Carolina Carvajal Guiral	Técnico Operativo	Técnico y administrativo
Liliana Maria Alvarez Gomez	Profesional Especializada (E)	Jurídico
Sandra Patricia Ángel Escobar	Profesional Universitario	Financiero

12. SUPERVISION.

La supervisión será ejercida a través del Director Administrativo de Desarrollo Tecnológico con el apoyo a la labor de supervisión, el cual será a través del servidor público que designe aquel, para lo cual, la Secretaría General formalizará la supervisión a través del respectivo memorando.

13. DECLARACION DE INHABILIDADES E INCOMPATIBILIDADES, CONFLICTOS DE INTERES COMO ACCION PARA ABORDAR EL RIESGO DE SOBORNO.

A través del presente documento los integrantes del equipo de trabajo dejamos constancia de no encontrarnos incursos en violación al régimen de inhabilidades e incompatibilidades para contratar ni conflictos de interés para adelantar las etapas que corresponden al presente proceso de contratación.