SELECCIÓN ABREVIADA POR SUBASTA INVERSA No. 9015926 de 2026

OBJETO:

Adquirir licencias, soporte y actualización para las soluciones de dispositivos de seguridad perimetral de nueva generación con IPS en alta disponibilidad

1. Denominación del bien o Servicio

HARDWARE, SOFTWARE, REDES Y ACCESORIOS

2. Denominación técnica del bien o Servicio

HARDWARE, SOFTWARE, REDES Y ACCESORIOS

3. Unidad de medida

UN

4. Descripción General

OBJETIVO GENERAL

Fortalecer los controles de seguridad informática del Distrito de Medellín a partir de la adquisición de licencias, soporte y actualización para las soluciones de dispositivos de seguridad perimetral de nueva generación con IPS en alta disponibilidad de las siguientes soluciones: una orientada a proteger la infraestructura tecnológica de las amenazas asociadas a la seguridad perimetral y la otra orientada a la protección de los servidores alojados en el centro de datos corporativo y a la protección de la interconexión con la red de las Secretarias de Seguridad y Movilidad para aportar a la mitigación de ataques informáticos especializados contra los servidores, sus sistemas operativos o los servicios que estos prestan.

OBJETIVO ESPECIFICO

Realizar las actividades relacionadas con el aprovisionamiento de las licencias de software requeridas y los servicios de soporte y actualizaciones del firmware, en el marco del proceso de contratación del Distrito de Medellín para las siguientes soluciones:

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

. Una solución de firewall de dispositivos de seguridad perimetral de nueva generación con IPS en alta disponibilidad para proteger la plataforma informática contra ciberataques debido a los servicios publicados en Internet,

. Y otra solución de firewall de Datacenter de nueva generación con IPS en alta disponibilidad que actualmente protege las conexiones desde y hacia el centro de datos corporativo principal, así como las conexiones que se establecen entre la red LAN operada por la Secretaria de Innovación Digital y las redes que las Secretarias de Seguridad y Movilidad opera de forma autónoma.

1. ESPECIFICACIONES TÉCNICAS

. Se debe proveer el licenciamiento, así como el servicio de actualización y soporte, tanto local como de fabricante, para las siguientes soluciones; una de dispositivos Firewall de seguridad perimetral y la otra Firewall de Datacenter e interconexión con las Secretarías de Seguridad y Movilidad que actualmente posee el Distrito de Medellín. El periodo de licenciamiento y servicio debe ser de un (1) año contado a partir de la fecha del inicio de ejecución por parte del supervisor a través de la plataforma Secop II del eventual contrato. Los dispositivos que involucran la solución, el licenciamiento y los servicios queridos para cada uno, son:

1.1. DISPOSITIVOS CISCO ISE 3615 (2 dispositivos físicos y 3 MV)

1.1.1 LICENCIAS Y SERVICIOS REQUERIDOS

· 5100 Licencias Cisco Identify Service Engine Essentials Subscription, por un (1) año. SKU: ISE-E-LIC.
· 600 Licencias Cisco Identify Service Engine Premier Subscription, por un (1) año SKU: ISE-P-LIC
· Soporte del fabricante:
Soporte Fabricante (Cisco) 7x24 para los dos (2) equipos físicos, Small Secure Network Server for ISE Applications, por un (1) año. SKU: CON-SNTP-SNS3615K.
Soporte Fabricante (Cisco) 7x24 para los tres (3) virtuales, Cisco ISE Virtual Machine Common PID, por un (1) año. SKU: CON-ECMU-RISE9KVM
· Soporte local:
Soporte Proveedor 7x24 para los cinco (5) ISE 3615 (2 físicos y 3 MV con su administración), por un (1) año. En los términos y ANS definidos más adelante.

1.2. DISPOSITIVOS CISCO FIREWALL 4115 (2 dispositivos)

1.2.1. LICENCIAS Y SERVICIOS REQUERIDOS

· 2 Licencias (1 para cada dispositivo) de funcionalidades IPS, Antimalware, Filtrado de contenido, Control de aplicaciones para Firewall Cisco FPR4115 (Threat Defense Threat, Malware and URL License), por un (1) año. SKU: L-FPR4115T-TMC-1Y
· 4000 Licencias AnyConnect Plus compatible con ISE para usuarios VPN, Secure Client Advantage Term License, Total Unique Users, por un (1) año. SKU: L-AC-PLS-1Y-S6
· 200 Licencias Cisco AnyConnect Apex License, por un (1) año. SKU: L-AC-APX-1Y-S3

· Soporte del fabricante:
Soporte Fabricante Cisco 7x24 para los dos (2) Módulos de tarjetas de red Cisco FirePower 8 port SFP+ Network Modul, por un (1) año. SKU: CON-SNTP-F4KNMX1G.
Soporte Fabricante (Cisco) 7x24 para los dos (2) Cisco Firepower 4115 NGFW Appliance, 1U, 2 x NetMod Bays, por un (1) año. SKU: CON-SNTP-FPR4115N
· Soporte local:
Soporte Proveedor 7x24 para los dos (2) Cisco Firepower 4115 NGFW, por un (1) año. En los términos y ANS definidos más adelante
· 2000 Cisco Dúo Essentials edition (formerly MFA), SKU: DUO-ESSENTIALS, Cisco Duo Basic Support, por diez (10) meses y veinte (20) días. SKU: SVS-DUO-SUP-B - Por tratarse de servicio en nube es excluido de IVA.

1.3. DISPOSITIVO CISCO FIREPOWER MANAGEMENT #FMC

1.3.1 SERVICIOS REQUERIDOS

· Soporte del fabricante:
Soporte Fabricante Cisco 7x24 Firepower Management Center virtual para VMware for 25 devices, por un (1) año. SKU: CON-ECMUS-SFFMCVKF.
· Soporte local:
Soporte Proveedor 7x24 para Firepower Management Center virtual para VMware for 25 devices, por un (1) año. En los términos y ANS definidos más adelante.

1.4. DISPOSITIVOS CISCO FIREWALL FPR4225 (2 dispositivos)

1.4.1 DISPOSITIVOS, LICENCIAS Y SERVICIOS REQUERIDOS

· 2 Licencias (1 para cada dispositivo) de funcionalidades IPS, Antimalware, Control de aplicaciones para Firewall 4225 Threat Defence and Malware1Y Subs, por diez (10) meses y once (11) días. SKU: L-FPR4225T-TM- 1Y
· 5 Transceiver SFP 28 (25 Gbps) Cisco, 25GBASE-SR SFP Module. SKU: SFP-25G-SR-S.
· Soporte del fabricante:
Soporte Fabricante Cisco 7x24 para los dos (2) módulos Cisco Secure Firewall 4200 8x25G ZSFP Netmod, SOLN SUPP 8x5xNBD CISCO SECURE FIRE POWER, por un (1) año. SKU:CON-SSSNT- FPR4KX25·
Soporte Fabricante Cisco 7x24 para los dos (2) Cisco Secure Firewall 4225 NGFW Appliance, 1U, 2xNetMod Bays, por un (1) año. SKU: CON-SNTP-FPR4225N
· Soporte local:
Soporte Proveedor 7x24 para los dos (2) Firewall 4225, por un (1) año. En los términos y ANS definidos más adelante.

1.5. DISPOSITIVOS CISCO FIREWALL 3105 (4 dispositivos)

1.5.1 LICENCIAS Y SERVICIOS REQUERIDOS

· 4 Licencias (1 para cada dispositivo) de funcionalidades IPS, Antimalware, Control de aplicaciones para Firewall 3105, Cisco Secure Firewall 3105 Threat Defence and AMP License, por un (1) año. SKU: L-FPR3105T-TM-1Y.
· Soporte del fabricante:
Soporte Fabricante Cisco 7x24 para los cuatro (4) Cisco Secure Firewall 3105 NGFW Appliance, 1U, por un (1) año. SKU: CON-SNTP-FPR3105N.
· Soporte local:
Soporte Proveedor 7x24 para los cuatro (4) Firewall 3105, por un (1) año. En los términos y ANS definidos más adelante.

1.6 ACTUALIZACIONES

· Actualización automática de definiciones de indicadores de compromiso.
· Recibir actualizaciones inmediatas de nuevas amenazas por el periodo contratado.
· La plataforma se debe mantener actualizada o migrada a nuevas versiones estables liberadas por el fabricante.
· Las actualizaciones y migraciones a otras versiones de la herramienta que sean necesarias deben ser informadas y los servicios prestados de instalación deben ser soportados por el contratista durante el periodo del contrato y deberán estar incluidas en el presupuesto.
· La plataforma deberá mantenerse en la última versión estable y se debe realizar acompañamiento para la migración.
· Las actualizaciones que sean necesarias para garantizar el uso eficiente serán prestadas por el contratista bajo su responsabilidad tanto de informarlas como de su instalación ya sea remotamente o en sitio.

1.7 REPORTES E INFORMES

· El módulo de reportes e informes debe estar incluido en la solución.
· Reportes predefinidos.
· Reportes de estado de actualización de definiciones.
· Las políticas, los cuadros de mando, informes y demás deberán estar disponibles en una consola o menú gráfico.
· Generación de informes dinámicos los cuales pueden ser diarios, semanales o mensuales teniendo disponibilidad de datos en archivos planos y envió automático del reporte.
· La solución debe de permitir exportar las políticas que se tengan implementadas mediante reportes (en excel, pdf, cvs, txt) teniendo en cuenta la prioridad de aplicación de las mismas.
· La solución deberá permitir generar reportes históricos.
· La solución deberá permitir generar reportes de las amenazas bloqueadas.
· La solución deberá tener la capacidad de enviar reportes programados por correo electrónico.

1.8 SOPORTE

· Soporte Local para los dispositivos, el proveedor deberá prestar el servicio de soporte de partner 7x24 sobre las soluciones de Firewall Perimetral con sus componentes: CISCO ISE 3615 (2

dispositivos físicos y 3 MV), CISCO NAC, CISCO APEX, CISCO FIREWALL 4115 (2 dispositivos), Módulos de tarjeta de red (2), y CISCO DUO, Firepower Management Center (FMC) virtual para VMware. Y de Firewall de Datacenter e interconexión con las Secretarías de Seguridad y Movilidad con sus componentes: CISCO FIREWALL 4225 (2 dispositivos), Módulos de tarjeta de red 8x25G SFP (2), CISCO FIREWALL 3105 (4 dispositivos), por el periodo de un (1) año, de acuerdo con la necesidad de la entidad, detallado en las especificaciones técnicas.

· Soporte por 12 meses para atención a los componentes listados en el numeral anterior.
· El servicio de soporte debe ser prestado por personal certificado en la solución, ubicado en Medellín o en el Área Metropolitana del Valle de Aburrá.
· En la atención de los casos de soporte se debe reportar el número de caso tanto del proveedor como del fabricante.
· No se pueden cerrar los requerimientos (Casos de Soporte # Tickets) hasta que el supervisor del contrato autorice.
· Realizar las visitas necesarias para la solución de incidentes, si la materialización de una incidencia a juicio del supervisor del contrato requiere de la intervención y participación presencial de personal especializado por parte de la empresa contratista, se debe contar con la disponibilidad de atención en sitio de acuerdo con la criticidad e impacto de la incidencia sobre la prestación del servicio, orientada a la recuperación del mismo.
· Las actividades de actualización que se requieran se deberán programar en horarios previamente autorizados por el Distrito de Medellín (horarios no laborales) y estos serán desarrollados por el contratista, quien deberá entregar el plan de trabajo respectivo.
· El servicio de soporte para los incidentes reportados debe ser atendido según los ANS.
· La atención vía telefónica, correo electrónico, soporte remoto y/o chat por parte del fabricante deberá garantizarse con disponibilidad 7x24, durante la vigencia del contrato.
· Las actividades de soporte debido a actualizaciones realizadas por el fabricante durante el periodo del contrato deberán estar incluidas en el presupuesto sin costo adicional para el Distrito de Medellín.
· Si la solución o herramienta posee problemas debe haber atención en sitio tiempo completo hasta que entreguen una solución real, confiable y estable.
· Servicio de soporte en sitio en la ciudad de Medellín, para solucionar eventos de tipo correctivo bajo demanda con un nivel de servicio, máximo de una hora entre la llamada y la atención.

2. GARANTIA DE LA SOLUCIÓN

· Cubrir las garantías pactadas en las especificaciones esenciales.
· Garantizar la prestación del servicio con las especificaciones de tipo técnico establecidas en el estudio previo y el pliego de condiciones definitivo.
· Garantizar la disponibilidad de las soluciones durante la vigencia del contrato.
· Garantía de 1 año, contado a partir de la fecha del inicio de ejecución por parte del supervisor a través de la plataforma Secop II, para todo el software adquirido y el hardware sobre el cual éste opera o se adquiera.
· En caso de reemplazo de hardware total o parcial, el envío debe gestionarse de manera inmediata a la notificación del Distrito de Medellín, teniendo en cuenta los acuerdos de niveles de servicio de remplazo de hardware del fabricante para entregarlo en las instalaciones del Distrito de Medellín; toda la gestión, gastos de envío, nacionalización y demás serán a cargo del contratista.
· Montar servidores virtuales como plan de contingencia, sin tener que pagar un licenciamiento

adicional, en caso de presentarse una falla total o parcial que afecte el servicio siempre y cuando lo amerite.
· Si por algún motivo se detecta que la solución tiene fallas en su hardware sobre el que operan las licencias de software adquiridas o el hardware que se adquiera, el contratista debe asumir totalmente los costos de cambio o actualización de ello como memoria, procesador, disco duro, fuente de energía u otros componentes.
· Los productos que sean entregados en virtud del contrato que se suscriba, como las actualizaciones de software para los equipos descritos y el hardware que se adquiera, deben contar con garantía por toda la vigencia del contrato, siendo responsabilidad del contratista reparar o corregir cualquier impacto negativo que la aplicación de estos productos tenga sobre los equipos, su desempeño o el servicio que prestan, sin que esto tenga costo adicional para el Distrito de Medellín.

3. ENTREGABLES

· Certificación de garantía de hardware y software por 1 año, plazo 15 días calendario a partir de la fecha del inicio de ejecución por parte del supervisor a través de la plataforma Secop II.
· Asignación del licenciamiento contratado mediante documento del fabricante de la solución que indique expresamente que se han asignado al Distrito de Medellín, incluyendo fecha de inicio y fecha final de la suscripción del licenciamiento y soporte, plazo 15 días calendario a partir de la fecha del inicio de ejecución por parte del supervisor a través de la plataforma Secop II.
· Plan de contingencia para la plataforma y restauración del sistema, plazo treinta (30) días calendario a partir de la fecha del inicio de ejecución por parte del supervisor a través de la plataforma Secop II.
· El contratista deberá suministrar datos de contacto para soporte y un instructivo de cómo generar los casos, plazo 8 días calendario a partir de la fecha del inicio de ejecución por parte del supervisor a través de la plataforma Secop II. Si algún canal para soporte cambia este documento debe ser actualizado inmediatamente.
· Cronograma de servicio de soporte preventivo incluida en la solución, plazo treinta (30) días calendario a partir de la fecha del inicio de ejecución por parte del supervisor a través de la plataforma Secop II.
· Documento que certifique fecha de inicio, terminación del soporte y actualización.
· Manuales y documentación actualizada de la última versión para la administración, configuración, parametrización e instalación de la solución implementada en el Distrito de Medellín, plazo 30 días calendario a partir de la fecha del inicio de ejecución por parte del supervisor a través de la plataforma Secop II.
· Las nuevas funcionalidades integradas en las actualizaciones deben ser notificadas y documentadas al supervisor del contrato.
· Entrega de informe cuatrimestral del estado de Salud de los equipos que conforman la solución de Perímetro y Datacenter, incluidos en el alcance del contrato.
·Temario y material de la transferencia de conocimiento.

Nota: Toda la documentación, transferencia de conocimiento, información, manuales y demás textos específicos generados en el marco del proyecto serán de propiedad del Distrito Especial de Medellín y deben estar escritos en español, los manuales de fabricante podrán ser entregados en el idioma inglés.

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

4. ACUERDOS DE NIVELES DE SERVICIO (ANS)

De acuerdo con su naturaleza, los incidentes de soporte con el hardware y/o software se pueden clasificar como: Crítica, Alta, Media, Baja, Negociada; por lo tanto, la atención será regida bajo las siguientes prioridades:

· Prioridad 1 (Critica): Procesos que afecten la prestación de servicios a la ciudadanía de la línea base administrada, evento que genere falla masiva en la prestación de un servicio de TI crítico, evento que afecte la prestación de algún servicio TI a usuarios del despacho del Alcalde. Tiempos de atención: 30 Minutos.
· Prioridad 2 (Alta): Evento que afecte la prestación de servicio TI a Puntos de atención a los usuarios internos (empleados del Distrito de Medellín) evento que afecte la prestación de algún servicio TI a Secretarios de despacho, subsecretarios o directores técnicos, Falla que afecte el servicio TI en aulas de capacitación, cuando se dicta una capacitación que afecte el tiempo comprometido por los usuarios, evento TI que impida el desarrollo total de las labores de un funcionario del Distrito de Medellín. Tiempos de atención: 40 Minutos.
· Prioridad 3 (Media): Evento TI que impida el desarrollo parcial de las labores de un funcionario del Distrito de Medellín. Tiempos de atención: 3 horas.
· Prioridad 4 (Baja): Instalación o reparación de software no crítico que no soporte las labores del usuario. Tiempos de atención: 12 horas.

5. MEDIOS POR DONDE SE PUEDE SOLICITAR UN SOPORTE TÉCNICO REQUERIDO POR EL DISTRITO ESPECIAL DE MEDELLÍN

Se debe desarrollar bajo los siguientes tipos de soporte dependiendo de su severidad:

· Soporte correo electrónico: Respuesta a través de un buzón de correo electrónico de soporte informado con anticipación, y deberá ser atendido de acuerdo con la criticidad del problema, si la dirección del buzón es modificada deberá ser informado este con anterioridad el cambio.
· Soporte telefónico: Si el número telefónico o los números telefónicos informados cambian, estos deben ser especificados con anterioridad, y deberá ser atendido de acuerdo con la criticidad del problema.
· Soporte Remoto: Para conectarse remotamente con el hardware, deberá contar con previa autorización por parte del líder de implementación de controles de la Secretaría de Innovación Digital, con el fin de garantizar la seguridad y control en el acceso.
· Soporte por chat: Deberá ser atendido de acuerdo con la criticidad del problema, si el chat es modificado deberá ser informado este con anterioridad el cambio.

6. OTRAS CONSIDERACIONES

· Las especificaciones técnicas requeridas son mínimas, por lo tanto, se pueden ofertar mejores características.
· La instalación deberá realizarse por personal certificado en la herramienta.
· Los gastos de envío, importación, instalación y demás que se generen con ocasión del reemplazo serán asumidos totalmente por el contratista.
· Las Actualizaciones que sean necesarias para garantizar el uso eficiente del hardware serán

prestadas por el contratista bajo su responsabilidad tanto de informarlas como de su instalación ya sea remotamente bajo las condiciones del numeral anterior o en sitio.
· El licenciamiento que se adquiera para los firewalls 4225, iniciará su vigencia una vez termine la implementación y entren en operación tanto el hardware como el software.

Nota:
Como las necesidades son mayores y los recursos son escasos, luego de finalizado el certamen de subasta, el valor obtenido como descuento se reinvertirá en Licencias Cisco DUO como parte de los componentes de la solución, por lo tanto, se adjudicará por el precio más cercano al presupuesto oficial.

7. TRANSFERENCIA DE CONOCIMIENTO

El proveedor deberá desarrollar sesiones de transferencia de conocimiento, donde a través de actividades de formación logre desarrollar en (10) funcionarios de la entidad habilidades y competencias enfocadas en los dispositivos o soluciones del objeto contractual; la sumatoria de horas de las sesiones debe ser de mínimo 24 horas, las cuales podrán realizarse de manera virtual y serán agendadas por el supervisor del contrato previa concertación con el proveedor.

REQUISITOS HABILITANTES

1. EXPERIENCIA GENERAL DEL PROPONENTE:

Para la verificación de la experiencia se tomarán los contratos ejecutados por el proponente, ya sea individualmente o en consorcio o unión temporal que estén registrados en el RUP, de los cuales el proponente deberá relacionar en el formato Experiencia del Proponente, aquellos con los que pretende acreditar las condiciones exigidas en este pliego. No se tendrán en cuenta para la evaluación los contratos que no estén registrados en el RUP.

Para ser considerado hábil el proponente deberá acreditar hasta cinco (5) contratos ejecutados, debidamente certificados en el Registro Único de Proponentes, identificados en el clasificador de bienes y servicios en el tercer nivel, en al menos uno de los códigos mencionados a continuación, cuyo objeto y/o alcance y/o actividades contemplen el componente de soporte o actualización de equipos de seguridad informática. La sumatoria de ellos deberán ser iguales o superiores a 100% del presupuesto oficial expresado en salarios mínimos mensuales legales vigentes SMMLV.

NIVEL	CÓDIGO	DESCRIPCIÓN
Clase	43233200	Software de seguridad y protección
Clase	81111800	Servicios de administración de sistemas y componentes del sistema
Clase	81112200	Mantenimiento y soporte de software
Clase	81112500	Servicio de alquiler o arrendamiento de licencias de software informático

PROPONENTE PLURAL

El proponente plural deberá acreditar experiencia en las condiciones indicadas anteriormente, mediante contratos debidamente certificados en el Registro Único de Proponentes (RUP) en los códigos solicitados.

El valor a acreditar por cada uno de los integrantes del consorcio, unión temporal u otra forma de asociación permitida por la ley, deberá corresponder a su porcentaje de participación en la forma asociativa y expresada en Salarios Mínimos Mensuales Legales Vigentes (SMMLV). En todo caso, cada integrante deberá acreditar como mínimo un (1) contrato, independientemente del número de integrantes de la forma asociativa. Si el proponente plural se conforma por un número mayor al número de contratos solicitados, el proponente informará cuales de los contratos aportados se deberán tener en cuenta para la verificación de la experiencia, sin perjuicio en todo caso de que, a cada uno de los integrantes de la forma asociativa, le corresponde acreditar un (1) contrato que corresponda a su porcentaje de participación en el correspondiente proponente plural.

EXPERIENCIA GENERAL DIFERENCIAL:

Con fundamento en el Artículo 2.2.1.2.4.2.18 respecto de las Mipyme, del Decreto 1082 de 2015, adicionado por el artículo 3 del Decreto 1860 de 2021, las Entidades Estatales establecerán condiciones habilitantes diferenciales que promuevan y faciliten la participación en los procedimientos de selección competitivos. En este sentido, para el presente proceso se establece el criterio diferencial descrito a continuación únicamente para la experiencia general:

Cabe aclarar que la aplicación de tal criterio diferencial no regirá en las convocatorias limitadas a Mipymes que se realicen conforme a los artículos 2.2.1.2.4.2.2 y 2.2.1.2.4.2.3 del Decreto 1860 de 2021.

EXPERIENCIA PARA MIPYME

De acuerdo con el artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, adicionado por el artículo 3 Decreto 1860 de 2021, el proponente individual o plural que cuente con la calidad de Mipyme deberá acreditar experiencia en las condiciones indicadas en la Experiencia General, no obstante, podrá acreditar experiencia hasta un contrato adicional al exigido, además, la sumatoria de estos contratos deberá ser igual o superior a 10% menos de lo exigido frente al presupuesto oficial expresado en salarios mínimos mensuales legales vigentes SMMLV.

ACREDITACIÓN DE CONDICIÓN DE MIPYME.

Para que un proponente, singular o plural, pueda acceder a criterios diferenciales para Mipyme en el presente proceso, deberá acreditar su condición de la siguiente manera:

i. Las personas naturales, mediante el formato Acreditación de Mipyme expedido por ellos y un contador público, adjuntando copia del registro mercantil, en el que se certifique el cumplimiento de los criterios para ser Mipyme, de conformidad con en el artículo 2.2.1.13.2.2 del Decreto 1074 de 2015.

ii. Las personas jurídicas mediante formato Acreditación de Mipyme expedido por el representante legal y el contador o revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación, en el que se certifique el cumplimiento de los criterios para ser Mipyme, de conformidad con en el artículo 2.2.1.13.2.2 del Decreto 1074 de 2015.

En todo caso, las Mipyme también podrán acreditar esta condición con la copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al cierre del proceso.

Para los casos de propuestas presentadas por Consorcios o Uniones Temporales, solo se aplicarán los criterios diferenciales si por lo menos uno de los integrantes acredita la calidad de Mipyme y tiene una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal.

ANOTACIONES GENERALES PARA LA EXPERIENCIA. Ver Pliego de condiciones

2. CERTIFICACIONES

El proponente deberá entregar con la propuesta los siguientes documentos:

· Security Partner: El proponente deberá acreditar certificación vigente como Partner autorizado del fabricante Cisco en el Portafolio de Seguridad (Security Partner), emitida directamente por el fabricante y vigentes al momento de la presentación de la oferta. Certificación que debe ser enviada directamente y a nombre del Distrito Especial de Medellín.

· Competencias asociadas: El proponente deberá contar con las competencias asociadas a Extended Detection and Response Competency y Secure Enterprise Infrastructure Competency, emitidas directamente por el fabricante y vigentes al momento de la presentación de la oferta. Certificación que debe ser enviada directamente y a nombre del Distrito Especial de Medellín.

3. AVAL DE LA PROPUESTA

De acuerdo con el artículo 20 de la Ley 842 de 2003, el representante legal o apoderado del proponente individual persona jurídica o el representante legal o apoderado de la estructura plural, debe acreditar que posee título como ingeniero de informática, ingeniero de sistemas, ingeniero de telecomunicaciones, ingeniero en telemática, para lo cual adjuntará copia de la tarjeta profesional y del certificado de la vigencia de matrícula profesional expedida por el COPNIA o Consejo Profesional en la respectiva rama de la ingeniería, según corresponda, con una vigencia no superior de 6 meses contados a partir de la fecha de cierre del Proceso de Contratación. El requisito de la tarjeta profesional se puede suplir con el registro de que trata el artículo 18 del Decreto - Ley 2106 de 2019.

En caso de que el representante legal o apoderado no posea título de una de las profesiones mencionadas, la oferta debe ser avalada por un ingeniero en las profesiones requeridas, para lo cual debe adjuntar los documentos solicitados.

4. PERSONAL MÍNIMO REQUERIDO

El Proponente debe contar con al menos con un (1) ingeniero certificado en CCNP Security o superior, que atienda el soporte técnico requerido. Este ingeniero debe estar ubicado en la ciudad de Medellín o en el Área Metropolitana del Valle de Aburrá con el fin de que pueda desplazarse a prestar soporte en sitio; cuando no se puede realizar conexión remota por algún inconveniente técnico y el caso de soporte lo amerite, sin afectar los ANS establecidos en los pliegos.

Para acreditar el cumplimiento de este requisito, el proponente deberá aportar debidamente diligenciado y firmado el Formato Compromiso De Cumplimiento Con El Personal Mínimo Requerido, suscrito por el representante legal, donde se evidencie el compromiso de contar con el personal en la ciudad de Medellín o en el Área Metropolitana del Valle de Aburrá.

5. ANEXO CUMPLIMIENTO FICHA TÉCNICA

El proponente deberá aportar el documento en mención, con lo cual se compromete con el cumplimiento de las especificaciones técnicas del bien o servicio de características técnicas uniformes y de común utilización.

OBLIGACIONES DEL CONTRATISTA

1. Cumplir con el soporte técnico, y mantenimiento de la plataforma de acuerdo a las especificaciones esenciales.
2. Atender los requerimientos solicitados por el supervisor del contrato, en el tiempo de respuesta establecido en los Acuerdos de Niveles de Servicio (ANS).
3. Garantizar los 12 meses de soporte iniciarán a partir de la entrega del licenciamiento que deberá darse al momento de la fecha del inicio de ejecución por parte del supervisor a través de la plataforma Secop II.
4. Comunicar al supervisor del contrato sobre algún cambio en el esquema de licenciamiento y éste no afectará el valor establecido del contrato. Así mismo, definir los planes de acción a implementar que se deriven de estos cambios. El contratista deberá hacerles seguimiento a estos planes de acción.
5. Presentar plan de contingencia de las soluciones objeto de la propuesta a contratar.
6. Contar con un plan para ajustarlo a las necesidades solicitadas inicialmente, en caso de presentar cambios en el esquema de licenciamiento, sin que ello incurra en costos adicionales a los adquiridos en la propuesta inicial.
7. Garantizar la prestación del servicio con las especificaciones de tipo técnico establecidas en el estudio previo y el pliego de condiciones definitivo.
8. Aceptar y firmar el acuerdo de confidencialidad entregado por el Distrito Especial de Medellín.
9. Cubrir las garantías pactadas en las especificaciones esenciales.
10. Cumplir con el objeto contractual dentro del plazo establecido para la ejecución del mismo.
11. Garantizar la disponibilidad de la solución durante la vigencia del contrato.
12. Presentar informe de las actividades realizadas durante la ejecución del objeto del contrato al funcionario encargado (supervisor) de ejercer la vigilancia y control del mismo para su correspondiente aprobación.
13. Cumplir oportunamente con los aportes al sistema general de seguridad social integral de conformidad con lo señalado en el artículo 50 de la Ley 789 de 2002, artículo 41 inciso 2- de la ley

80 de 1993 modificado por el artículo 23 de la ley 1150 de 2007, Ley 1562 de 2012 y demás normas concordantes, obligándose desde la celebración del contrato y durante toda su vigencia a efectuar los aportes al sistema General de seguridad Social (salud, pensión, riesgos laborales), así como los aportes parafiscales (siempre que aplique).
14. Contar con un Coordinador o Administrador quien será el enlace con el Distrito Especial de Medellín, para prestar atención personalizada a los requerimientos y/o dudas que se presenten en el desarrollo del contrato, según los canales de soporte descritos en las especificaciones técnicas.
15. Velar por conservar las configuraciones que recomiende el fabricante y por un uso óptimo de la plataforma en cuanto a sus funcionalidades.
16. Validar periódicamente el licenciamiento y las mejoras a este, con el propósito de que el Distrito Especial de Medellín no viole en ningún momento un incumplimiento por ello.
17. Las demás que se deriven de la naturaleza del contrato y que garanticen su cabal y oportuna ejecución.
18. Plantear acciones de mejora a las plataformas existentes en la Alcaldía de Medellín y el Conglomerado público para generar sinergia en los procesos y en los sistemas de la entidad.

OBLIGACIONES DEL CONTRATISTA REFERENTE AL CUMPLIMIENTO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO (SG-SST)

El contratista debe cumplir las disposiciones contempladas en el Decreto 1072 de 2015 y la Resolución 0312 de 2019 y las demás disposiciones vigentes en materia de Seguridad Social y Seguridad y Salud en el Trabajo. Esta obligación será verificada por los supervisores o interventores según aplique, con los siguientes documentos:

· La Autoevaluación del SGSST o autoevaluaciones del año en curso. Conforme a los resultados de la autoevaluación que aporte el contratista, éste asume unas obligaciones que están expresas en el artículo 28 Resolución 0312 de 2019, las cuales serán verificadas por el supervisor según sea el caso.
· Plan de Trabajo del SG-SST acorde a la autoevaluación o autoevaluaciones del año en curso.
· En los contratos donde el contratista deba dotar de elementos de protección personal, el supervisor debe constatar en campo dicha obligación, y solicitar al contratista formato de entrega de los elementos de protección personal que lleve la firma de los trabajadores que están prestando sus servicios en el Distrito Especial de Medellín, dejando todas las evidencias en el informe parcial de supervisión, y debe ser revisada en cada pago.

OBLIGACIONES DEL DISTRITO

1. Cancelar al contratista el valor del contrato, de acuerdo con la forma de pago establecida, previa presentación de las facturas o documentos equivalentes debidamente legalizados con todos los soportes que aseguren que los bienes o servicios fueron recibidos a entera satisfacción por parte del supervisor.
2. Asignar supervisor para vigilar el desarrollo y ejecución del contrato.
3. Suministrar la información que requiera EL CONTRATISTA en ocasión a la ejecución del presente contrato.
4. Informar y supervisar la solución de los incidentes o soportes.

5. Entregar la información requerida por el Contratista de manera oportuna.
6. Verificar el cumplimiento del pago de salarios, honorarios y demás obligaciones laborales, así como los aportes al sistema de seguridad social integral conforme a lo señalado en el artículo 50 de la Ley 789 de 2002 y normas reglamentarias.
7. Velar por el Cumplimiento de las disposiciones contempladas en el Decreto 1072 de 2015, la Resolución 0312 de 2019 y las demás disposiciones vigentes relacionadas con el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) por parte del contratista.
8. Verificar que, durante toda la ejecución del contrato, el contratista aplique las medidas necesarias de protección de todos los trabajadores
9. Verificar el cumplimiento por parte del contratista de las disposiciones relacionadas con el adecuado tratamiento de la información y de los datos sensibles de los cuales pudiere conocer con ocasión de este contrato, de acuerdo a lo señalado en los artículos 5 y 6 de la Ley 1581 de 2012.

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia