Radicado Interno: 2020002278

ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

1. NECESIDAD:

Uno de los objetivos principales del proceso de Gestión de Tecnología de Información de la Empresa para la Seguridad Urbana – ESU, es propender por la actualización y renovación tecnológica de modo que se puedan suplir las necesidades misionales de la empresa. Para cumplir con estos objetivos, la Oficina Estratégica procura mantener y optimizar los activos de tecnología a través de planes de mejoramiento continuos basados en actividades inherentes a la operación y soporte (atención de necesidades, solución de fallas, actualizaciones, optimizaciones, implementaciones y en general, la puesta a punto de los servicios de infraestructura tecnológica de la entidad) dentro de una línea de eficiencia administrativa y austeridad del gasto (Costo\Eficiencia).

Con el fin de contar con los servicios de instalación, administración y mantenimiento de la plataforma de seguridad informática de la ESU, la cual incluye el licenciamiento, dispositivos, soporte, mantenimiento y puesta a punto de dicha plataforma a través de la implementación de herramientas, funciones, políticas y controles de seguridad requeridos (Ej. antivirus, antimalware, gestión de puertos USB) que permitan disminuir posibles riesgos y prevenir cualquier tipo de ataque a la infraestructura y sistemas de información de la entidad, garantizando con esto disponibilidad, integridad y confiabilidad de su información; máxime en estos momentos de alto riesgo en los cuales se vienen realizando ataques informáticos persistentes de clase mundial a través de algunos virus tipo Ransomware (Algunos como: WannaCry, Petya, otros) se requiere contratar una solución de seguridad hasta el 30 de junio del año 2020.

El plazo anterior enmarcado en la actual crisis de los mercados mundiales debido a los esfuerzos que adelantan los diferentes gobiernos, buscando mitigar el efecto del coronavirus (COVID-19) en sus ciudadanos. Este problema mundial ha llevado a tener una tasa representativa del mercado alta, la gran mayoría de los productos de TI son transados en moneda Estadounidense USD (Dólar Americano) y siendo consecuentes con la línea de eficiencia administrativa, se busca adquirir la solución de la infraestructura y sistemas de información de la entidad, al menor tiempo posible y a un menor precio, esperando en un futuro cercano, un equilibrio de las economías mundiales, que le permitan a la moneda local COP (Peso Colombiano) adquirir valor frente al dólar para poder adquirir productos con una tasa más competitiva.

La contratación de los servicios tecnológicos deberá garantizar la disminución de riesgos asociados a la intervención y manipulación de la información de la entidad, la continuidad del servicio, administración, conocimiento y acceso a la plataforma informática de la entidad; lo que de no gestionarse expondría innecesariamente a la entidad a ataques por fallas o explotación de vulnerabilidades, máxime, cuando la mayoría de los funcionarios de la entidad debido a la pandemia y a la orden del Gobierno Nacional, Departamental y Municipal se encuentran

ejerciendo sus funciones bajo la figura de Trabajo en Casa", y es en estos casos donde la información puede ser más vulnerable.

Teniendo en cuenta lo anterior, el propósito de esta contratación es mantener la continuidad del servicio de seguridad informática instalada, la cual hoy se encuentra en óptimas condiciones y enmarcada bajo la norma ISO 27001:2013. En la actual vigencia se cuenta con el presupuesto necesario para contratar esta solución.

2. OBJETO:

Prestación de servicios para el aprovisionamiento, administración y mantenimiento (instalación, actualización, configuración, soporte y puesta a punto) de la solución de seguridad informática de la ESU, basada en licenciamiento Antivirus y dispositivos Fortinet.

3. ESPECIFICACIONES DEL BIEN O SERVICIO A CONTRATAR:

Para la solución de seguridad de la ESU, se establecen 3 componentes de servicio principales que son:

Tipo	Producto	Cantidad
Antivirus	Kaspersky Endpoint Security for Business Advanced x 3 meses	101
Firewall	Licenciamiento Fortinet UTM x 3 meses	2
Soporte técnico	Especializado y Mantenimiento para firewall y antivirus x mes	3

3.1 Licenciamiento de Antivirus x 3 meses

Renovación de licencia de software antimalware y de seguridad Endpoint Kaspersky Endpoint Security for Business Advanced para estaciones, servidores y equipos portátiles físicos, compatibles con el licenciamiento actualmente instalado en la entidad

- 45 equipos físicos, entre equipos de escritorio, portátiles con Windows y mac
- 50 escritorios virtuales con Windows 10
- 6 licencias variables para servidores de prueba y de uso del área de TI

Debe incluir: Actualizaciones de definiciones de malware y nuevas versiones del software durante 3 meses y Soporte técnico 8 x 5 por Internet durante 3 meses del fabricante

3.2 Licenciamiento Fortinet x 3 meses

Renovación, mantenimiento, garantía de hardware y soporte técnico de los módulos de protección del dispositivo perimetral, antimalware y filtrado de contenido web para:

- 2 Dispositivos en HA - Fortigate UTM (Appliance 90D)

Debe incluir: Mantenimiento y soporte técnico de segundo nivel 7 x 24 durante 3 meses por parte de FORTINET. Garantía de hardware por parte del fabricante durante 3 meses.

3.3 Soporte técnico especializado y mantenimiento:
Monitoreo, administración y soporte técnico avanzado del sistema de seguridad informática multinivel de la ESU en horario 7 x 24 durante 3 Meses para el licenciamiento de Kaspersky y 26 meses para la administración de los Fortigate 90D. Sin límite de horas.

Debe incluir:

- Monitoreo y administración de la plataforma (todos los aplicativos de seguridad) en horario 5x8.
- Envío de notificaciones por email a los administradores de la ESU.
- Alertas tempranas ante nuevas amenazas, inteligencia día cero para comportamientos de virus, malware, worms, exploits y ataques de seguridad.
- Información detallada y recomendaciones sobre las medidas necesarias para responder ante nuevas amenazas y riesgos particulares de los sistemas de la ESU.
- Generación y envío mensual de reportes y gráficas del estado de la plataforma de seguridad Firewall que permitan informarse sobre la navegación de usuarios, ancho de banda y aplicaciones, uso web, correos, amenazas, uso VPN (De ser requerido), eventos del sistema, entre otros que puedan entregar el mayor detalle posible estableciendo un top para:
  - Uso de ancho de banda
  - Numero de sesiones
  - Estadísticas de tráfico
  - Categorías web
  - Categorías más bloqueadas
  - Categorías más visitadas
  - Categorías de aplicación x ancho de anda
  - Sitios web permitidos
  - Sitios web bloqueados
  - Sitios más visitados
  - Sitios x ancho de banda
  - Sitios x tiempo de navegación
  - Origen de las visitas
  - Búsquedas de usuarios
  - Usuarios visitantes y/o navegantes
  - Usuarios más activos
  - Usuarios más bloqueados
  - Usuarios x ancho de banda y sesiones
  - Usuarios x tiempo de navegación
  - Tiempos de navegación (en línea)
  - Tráfico de aplicaciones x ancho de banda
  - Tráfico de aplicaciones x sesiones
  - Direcciones IP o host destinos x ancho de banda

- Direcciones IP o host destinos x sesiones
- Equipos con mayor envío de correos
- Equipos con mayor recepción de correos
- Eventos y/o amenazas por posibles virus, spam, ataques o intrusiones identificadas.

- Generación y envío mensual de la gestión de antivirus (antimalware) que permitan informarse sobre:
  - Estado general de protección de los equipos en la red
  - Equipos infectados
  - Infecciones más comunes y recomendaciones de prevención
  - Equipos desinfectados en el mes
  - Informe de errores
  - Informe de uso de licenciamiento
  - Informe de protección de los equipos virtuales y físicos.

- Generación y envío mensual de la gestión de análisis de vulnerabilidades y distribución de actualizaciones que permitan informarse sobre:
- Equipos con actualizaciones instaladas y/o pendientes de sistema operativo básicas y críticas, service pack, entre otras externas como java, adobe, flash y demás.
  - Actualizaciones recomendadas x equipo
  - Equipos más vulnerables
  - Informe de puertos abiertos
  - Informe de aplicaciones instaladas no autorizadas y/o gratuitas no permitidas.
  - Informe oportuno en el momento de identificar y/o presentar incidentes de seguridad.
  - Informe de vulnerabilidades en la red.
  - Análisis del riesgo de acuerdo a las políticas de seguridad implementadas para identificar vulnerabilidades y dar las recomendaciones necesarias.
- Reunión presencial o virtual (entre 1 a 2 veces al mes, presencial en caso de requerirse), de un ingeniero certificado en cada plataforma para solución de requerimientos, incidentes y reunión de coordinación con los administradores de la Plataforma de la ESU para realizar seguimiento y control del proyecto.
- Configuración en alta disponibilidad de los dos dispositivos Fortinet.
- Configuración de reglas y políticas de seguridad a nivel de Firewall para filtrar el tráfico que entra y sale de la Organización.
- Analizar e interpretar patrones de tráfico en conjunto con técnicas de detección heurísticas para detener posibles ataques antes de que sean efectuados (IPS/IDS).
- Antivirus a nivel del UTM, con detección de amenazas sobre los tipos de tráfico más comunes (SMTP, FTP, HTTP para garantizar una navegación segura en los usuarios de la Organización.
- Definir e implantar categorías de filtrado y parámetros requeridos para gestionar los permisos de acceso y navegación que realizan los usuarios de la ESU.

- Permitir y garantizar al momento que se requiera la configuración de conexiones VPN de tipo Site to Site y/o Client to Site.
- Aplicar las configuraciones necesarias en los distintos componentes de HW y SW que hagan parte de la solución y permitan su optimización.
- Identificación, análisis y control de vulnerabilidades a través de la herramienta correspondiente y entrega temprana de recomendaciones para tratarlas.
- Gestión de incidentes, cambios, configuraciones y operación.
- Debe atenderse y resolverse todos los incidentes y las solicitudes de servicios reportados, así como aquellos casos que puedan implicar instalación, configuración, actualización, monitoreo y administración de componentes de la solución y/o plataforma de seguridad informática para la ESU.
- Debe atenderse y resolverse todos los incidentes en horario 7x24.
- Debe atenderse las solicitudes de servicio reportadas en horario 5x8.
- Debe atenderse y resolverse en sitio aquellos casos que se no logren remotamente.
- Debe permitirse acceso de administrador al personal de TI de la ESU en el sistema o herramientas de administración de la seguridad.
- Ayudar a generar la matriz de riesgo de información según el informe entregado por la entidad externa que sea contratada para realizar las pruebas de ethical hacking, test de penetración e ingeniería social.
- Envío de reportes específicos solicitados en caso de requerirse.

Niveles de servicio: Disponibilidad: 99.6%, se excluye cualquier imputación al proveedor por fallas eléctricas de la ESU o fallos físicos en equipos que no hagan parte de la solución.

Disponibilidad	100 – 99,6 %	99,59 – 99 %	98,9 – 97 %	96,9 – 95 %	94,9 – 70%
Penalidad	0 %	5 %	10 %	15 %	30 %
Una indisponibilidad inferior al 70%, deberá ser negociada entre el supervisor y el prestador del servicio.					

Tiempos de atención y solución:

- Atención y diagnóstico de incidentes: 1 hora.
- Solución de incidentes: Según tabla (90% bajo la definición de nivel de criticidad: Critico, Alto, Medio, Bajo; el 10% restante en 12 horas).
- Ventanas de mantenimiento programadas: Deberán ser comunicadas por lo menos con 2 días de anticipación.

Definición niveles de criticidad para la atención y solución de casos:

Nivel de criticidad del incidente	**Critico**	**Alto**	**Medio**	**Bajo**
Definición de incidentes	Todos los equipos y	Algunos equipos y usuarios de la	Algunos equipos y usuarios de la	Un solo usuario afectado por

Nivel de criticidad del incidente	Critico	Alto	Medio	Bajo
	usuarios de la ESU sin disponibilidad de servicio. No es posible utilizar los sistemas que soportan los procesos del negocio	ESU se encuentran sin disponibilidad de servicio. Los sistemas que soportan los procesos del negocio están disponibles de forma intermitente para algunos usuarios	ESU se encuentran sin disponibilidad de servicio pero los sistemas que soportan los procesos del negocio se encuentran operativos	alguna configuración de seguridad. Los sistemas que soportan los procesos del negocio se encuentran operativos
Tiempo máximo de atención y solución	1 hora.	2 horas.	4 horas.	4 horas.

4. IDENTIFICACIÓN DEL TIPO DE CONTRATO A CELEBRAR:

Contrato de compraventa para el licenciamiento Antivirus y dispositivos Fortinet.
Contrato de prestación de servicios para el soporte técnico especializado y mantenimiento.

5. MODALIDAD DE SELECCIÓN DEL CONTRATISTA:

El presente proceso de contratación se fundamenta en la normatividad vigente para la contratación directa específicamente en la causal señalada en el artículo 24 del reglamento de contratación literal c), por tratarse de un Contrato de compraventa y actualización de tecnologías de la información que presentan compatibilidad con los actualmente implementados, el cual establece:

"Los contratos que tengan por objeto adquirir equipos de telecomunicaciones, equipos y/o tecnologías de la información, conocimiento científico o cuando se trate de compraventa, actualización, ampliación, modificación, o soporte de software o licencias de uso que presenten compatibilidad con los ya instalados o cuando los equipos y/o servicios estén sujetos a garantías de fábrica o exclusivas."

Se realiza estudio de mercado con diferentes proveedores, como lo son: IT SECURITY CONSULTORES, NSIT, TECHNOLOGY PARTNERS Y CLARO, de los cuales solo se obtuvo cotización efectiva y de los productos solicitados de los proveedores IT SECURITY CONSULTORES Y CLARO,

de los demás proveedores no se ha obtenido respuesta, o han ofertado productos diferentes a los solicitados, y que no son compatibles con los instalados en la entidad.

Por lo expuesto en la necesidad de optimización del gasto, las licencias de los productos deben pagarse one time a la firma del contrato, ya que es requerido por los fabricantes para la expedición de la misma y debido a la alta TRM vigente en estos momentos de contingencia no sería responsable con la búsqueda de una adecuada optimización de los costos adquirir el licenciamiento por un periodo mayor y teniendo en cuenta que debido a la anormalidad económica y laboral por la que atraviesa el país en este momento, no ha sido posible tener una pluralidad de oferentes que permita competir en igualdad de condiciones con diferentes proveedores del mercado.

Por todo lo anterior, es necesario realizar la contratación directa con el proveedor IT SECURITY CONSULTORES por un plazo de tres (3) meses, iniciando el primero (1) de abril de 2020; lo anterior dado que fue el único proveedor que presentó la cotización que se ajusta a las necesidades de la entidad, tiendo en cuenta que el plazo necesario es de Tres (3) meses y buscando una recuperación de la economía del país, en el cual se pueda realizar una contratación por un periodo aún mayor, que permita un adecuado ahorro por economía de escala.

6. VALOR ESTIMADO DEL CONTRATO Y JUSTIFICACIÓN DEL MISMO:

6.1 ESTUDIO DEL MERCADO:

Los proveedores que enviaron información para estudios previos fueron:

No.	OFERENTE	VALOR
1	IT Security Consultores	$ 11.964.736
2	Claro	$ 27.616.210

Nota: El valor de Claro fue calculado por prorrateo, ya que el periodo mínimo de contratación que ofrecen es de doce (12) meses, por lo que se realizan los cálculos a tres (3) meses con los valores por mes de un contrato anual.

6.2 VALOR ESTIMADO DEL CONTRATO

El valor del contrato es por la suma de **ONCE MILLONES NOVECIENTOS SESENTA Y CUATRO MIL SETECIENTOS TREINTA Y SEIS PESOS M.L.** ($*11.964.736*) incluido IVA y todos los costos directos e indirectos, tasas y contribuciones que conlleve la celebración y ejecución total del contrato que resulte del presente proceso de contratación el cual se desglosa de la siguiente manera:

Teniendo en cuenta que la contratación tiene 2 componentes, el licenciamiento es en dólares americanos y los cuales calculados con una TRM de $4.300

Producto	Total IVA incluido USD	TRM	Total IVA incluido Pesos
Antivirus	961,52	$4.300	$ 4.134.536
Firewall	714	$4.300	$3.070.200

El componente de soporte es valorado en pesos y tiene el siguiente valor

PRODUCTO	VALOR UNITARIO IVA	MESES	TOTAL IVA INCLUIDO
Soporte y mantenimiento Antivirus	793.333,33	3	$2.380.000
Soporte y mantenimiento Firewall	793.333,33	3	$2.380.000
		Total	**$4.760.000**

6.3 INFORMACIÓN PRESUPUESTAL QUE RESPALDA LA CONTRATACIÓN

Con base en el anterior sondeo de mercado, la ESU cuenta con el presupuesto para dicha contratación que se deberá ejecutar de la siguiente manera:

Componente	Rubro	Centro de Costos
Antivirus	12060402-1	13938
Firewall	12060402-1	13438
Soporte y Mantenimiento Antivirus	12060402-1	13938
Soporte y Mantenimiento Firewall	12060402-1	13438

7. JUSTIFICACIÓN DE LOS FACTORES DE SELECCIÓN*:*

- Cumplimiento de las especificaciones técnicas del numeral 3 del presente documento
- Menor precio ofertado.

8. RIESGOS: Ver matriz de riesgo anexa en archivo Excel.

9. GARANTÍAS EXIGIDAS: análisis que sustenta la exigencia de garantías.

DESCRIPCIÓN	PORCENTAJE DEL VALOR TOTAL DEL CONTRATO	DURACIÓN
Calidad del servicio y de los bienes y equipos	20%	Igual a la vigencia del contrato y seis (6) meses más
Cumplimiento del contrato	20%	Igual a la vigencia del contrato y seis (6) meses más

Pago de salarios, prestaciones sociales e indemnizaciones laborales	10%	Igual al plazo del contrato y tres (3) años más

10. INDICACIÓN DE SI LA CONTRATACIÓN RESPECTIVA ESTÁ COBIJADA POR UN ACUERDO INTERNACIONAL O UN TRATADO DE LIBRE COMERCIO VIGENTE PARA EL ESTADO COLOMBIANO:

La contratación no está cobijada por Acuerdo Internacional o Tratado de Libre Comercio.

11. CONDICIONES CONTRACTUALES:

11.1 OBLIGACIONES DEL CONTRATO

11.1.1 OBLIGACIONES DE LA ESU:

1) Exigir al contratista la ejecución idónea y oportuna del objeto contratado.
2) Actualizar y adoptar las medidas necesarias cuando se produzcan fenómenos que alteren en su contra el equilibrio económico o financiero del contrato, previo informe del supervisor, sobre la ocurrencia de tales hechos
3) Adelantar las acciones conducentes a obtener la indemnización de los daños que sufran en desarrollo o con ocasión del contrato.
4) Repetir contra los empleados de la ESU, el contratista o terceros, por las indemnizaciones que deban pagar, como consecuencia del presente contrato.
5) Pagar oportunamente al contratista el valor del contrato, de conformidad con lo establecido en la cláusula quinta.
6) Prestar al contratista todo lo necesario para la adecuada ejecución del objeto contractual.

11.1.2 OBLIGACIONES ESPECIFICAS DEL CONTRATISTA:

El contratista por su lado y en desarrollo del presente contrato tendrá los siguientes derechos y obligaciones:

1) Recibir oportunamente el pago estipulado en la cláusula quinta de este contrato.
2) Cumplir de buena fe con el objeto del presente contrato, de conformidad con la propuesta adjunta, la cual hace parte integral del contrato.
3) Designar un representante para efectos de facilitar y agilizar el manejo de la información entre las partes.
4) Presentar los informes requeridos sobre la ejecución del contrato.
5) Presentar las observaciones y recomendaciones para el buen desarrollo del contrato.
6) Cumplir con el objeto contractual acordado en la forma, cantidad, lugar, fechas y especificaciones requeridas por la ESU.
7) Constituir las garantías que le sean exigidas en el presente contrato y mantenerlas vigentes por el tiempo estipulado por la ESU.

8) Acreditar el pago de salarios, aportes parafiscales y seguridad social para cada uno de los pagos.
9) Acatar los requerimientos y observaciones que con ocasión de la ejecución del contrato le hagan el supervisor y/o la contratante.
10) Las demás que tengan relación directa con la naturaleza y objeto del presente contrato...)

11.1.3 PRODUCTOS Y/O SERVICIOS:
Ver detalle en numeral 3. ESPECIFICACIONES DEL BIEN O SERVICIO A CONTRATAR

11.1.4 FORMA DE PAGO:
La ESU pagará al Contratista mediante un pago único los licenciamientos de antivirus y firewall por un valor de USD 1675,52 liquidados a la TRM del día, y en tres (3) Pagos iguales mes vencido, contra entrega de servicio demandado por la ESU y efectivamente prestado, luego de recibidos los informes de ejecución del contrato, a partir del primero (1) de abril.

11.1.5 SUPERVISIÓN DEL CONTRATO: La Supervisión del Contrato estará a cargo de PROFESIONAL UNIVERSITARIO GRADO 2 - OFICINA ESTRATÉGICA o quien haga sus veces o quien designe el Ordenador del Gasto; el cual ejercerá las obligaciones y responsabilidades de acuerdo con lo establecido en el Manual de Contratación de la Entidad.

11.1.6 PLAZO DE EJECUCIÓN: Desde primero (1) de abril hasta el (30) de junio de 2020, previa aprobación de las garantías de cumplimiento por parte de la Secretaría General.

11.1.7 LUGAR DE EJECUCIÓN DEL CONTRATO: El objeto del contrato se ejecutará en la ciudad de Medellín.

Cordialmente,

DANIEL ESTEBAN MONTAÑO LÓPEZ
Profesional Universitario G2 – Oficina Estratégica

ALEJANDRO DE JESÚS ROJAS MEDINA
Jefe Oficina estratégica