ESTUDIOS PREVIOS - DIRECTA
CAUSAL IGUAL O INFERIOR A 150 SMMLV

1.- NECESIDAD Y CONVENIENCIA

El Decreto 1258 del 17 de junio de 2013 señala que la Unidad de Planeación Minero-Energética -UPME es una unidad administrativa especial de carácter técnico, adscrita al Ministerio de Minas y Energía, con personería jurídica, patrimonio propio y régimen especial en materia de contratación.

De conformidad con lo definido en el Decreto 1258 de 2013, es responsabilidad de la Oficina de Gestión de Información (OGI) de la Unidad de Planeación Minero Energética – UPME Preparar, divulgar y custodiar la información y estadísticas del sector minero y energético en los diferentes medios de divulgación, de conformidad con las directrices impartidas por la Dirección de la Unidad; así mismo desde la OGI se Coordina y administrar el sistema de información sectorial y sus subsistemas, con el fin de garantizar la disponibilidad, la integridad y la confiabilidad de la información, haciendo uso de la información que deben entregar las entidades del sector, de conformidad con el Decreto número 4130 de 2011 y demás normas que lo modifiquen o sustituyan, además se debe velar por el adecuado y óptimo funcionamiento de la plataforma tecnológica de la Unidad, garantizando los sistemas de seguridad y gestión de la información entre otras funciones.

La UPME y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes inherentes a los activos de información, pueden someter a los mismos a diversas formas de fraude, espionaje, sabotaje o vandalismo, entre otros. Los virus informáticos, el "hacking" o los ataques de negación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallas técnicos. Es por ello que se debe brindar protección al ecosistema tecnológico de la Unidad para proteger y asegurar la continuidad del negocio y minimizar el daño que pueda sufrir la organización debido a una situación adversa sobre sus activos tecnológicos o bienes de información, mediante la prevención y disminución del impacto de los incidentes de seguridad.

Que el Gobierno Nacional, a través del CONPES 3854 de 2016, define la Política de Seguridad Digital, para abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales; incluyendo la gestión del riesgo como uno de los elementos más importantes para abordar esta política.

Que con el fin de dar cumplimiento a las anteriores previsiones y a lo ordenado por los literales a) y f) del artículo 2 de la Ley 87 de 1993, artículo 2, literales a y f, en cuanto a la protección de los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten así como la definición y aplicación de medidas para prevenir los riesgos; detectar y corregir las desviaciones que se presentan en la organización y que puedan afectar el logro de sus objetivos, se hace necesario disponer lo pertinente al interior de la UPME.

Que la utilización de tecnologías en el procesamiento, almacenamiento, recuperación y transmisión de la información implica importantes riesgos para su disponibilidad, confidencialidad e integridad; estos atributos se deben asegurar en cumplimiento de las labores de apoyo, seguimiento y mejora continua del SGSI y por tanto es importante contar con plataforma tecnológica para la protección de la información y de

la plataforma tecnológica de la Unidad y en este sentido contar con una solución de Endpoint es necesario como primera línea de defensa del ecosistema digital de la UPME, lo anterior debido a que el 70% de las vulneraciones de datos exitosas comienzan en los EndPoint o equipos finales de una red de datos.

Por lo anterior, en la Unidad se requiere contar con una solución de seguridad digital a nivel de EndPoint, que apoye la Gestión Integral de la Seguridad Informática, que integre un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, logrando, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

La presente contratación fue aprobada en Comité de Contratación del 30 de mayo de 2023.

2.- OBJETO

Adquirir una solución Endpoint antivirus para la UPME.

3.- OBJETIVOS ESPECIFICOS

- Adquirir el licenciamiento de una solución tipo MDR Complete de Sophos (Licenciamiento XDR + SOC) para protección antimalware de computadores y servidores de la Unidad que cuente con servicio de monitoreo 24x7 de caza y respuesta ante amenazas (SOC) para 350 dispositivos de cómputo por 1 año.
- Adelantar el proceso de instalación, configuración y puesta en producción de la solución adquirida en los 4 días calendario siguientes a la firma del contrato.
- Contar con las actualizaciones permanentes que libere el fabricante de la solución adquirida.
- Realizar transferencia de conocimiento hacia la Unidad en los términos del anexo técnico y la oferta presentada por el proveedor.
- Prestar el respectivo soporte técnico de la solución que permita: Prevenir, detectar y neutralizar software malicioso, a través de tres componentes a saber: prevención de intrusos, antimalware y firewall usado con filtro de conexiones entrantes y salientes, en los términos del anexo técnico emitido por la Unidad, así como de la oferta presentada por el proveedor.
- Cumplir con el anexo técnico presentado y la oferta presentada.

4. OBLIGACIONES ESPECÍFICAS Y/O PRODUCTOS DEL CONTRATISTA

- Entregar las 350 licencias del XDR (Endpoint Extendido) de Sophos para la protección de computadores (190 licencias) y servidores (160 licencias) de la unidad.
- Instalación y configuración del licenciamiento adquirido en la plataforma tecnológica de la Unidad dentro de los 4 días calendario siguientes a la firma del contrato.
- Servicio de monitoreo 24x7 de caza y respuesta ante amenazas (SOC) para la plataforma tecnológica de la Unidad, incluidas las 350 licencias adquiridas en este proceso de contratación por 1 año.
- Garantía y soporte técnico de fábrica por un (1) año.
- Soporte local por un (1) año de acuerdo con el anexo técnico.
- Transferencia de conocimiento en los términos del anexo técnico de la oferta del proveedor.
- Entrega a satisfacción de la Unidad minero energético de los productos y servicios prestados.

Entrega de bienes

El contratista deberá entregar el siguiente bien tangible o intangible 350 licencias MDR Complete de Sophos (350 licencias de XDR + Servicio SOC), el cual se deberá ingresar a almacén.

5. OBLIGACIONES GENERALES DE LAS PARTES

Del Contratista:

- Cumplir el objeto del contrato/orden.
- Cumplir con las condiciones y lineamientos ofertados en la propuesta.
- Ejecutar el contrato/orden dentro del plazo establecido, y bajo las condiciones técnicas y financieras definidas en el presente proceso.
- Presentar cuenta de cobro o facturación electrónica, si por ley está obligado a ello, dentro de los plazos definidos en el contrato/orden.
- Mantener vigente y al día durante la ejecución del contrato la afiliación y aportes al sistema Integral de Seguridad Social Integral, Parafiscales y Sistema General de Riesgos Laborales. Está obligación no será exigible si el contratista o proveedor es una persona jurídica o natural extranjera.
- Constituir y modificar la garantía única de cumplimiento, si hay lugar.
- Las demás que le sean asignadas por el supervisor del contrato, en el marco del contrato/orden.

De la UPME:

- Designar el supervisor del contrato/orden.
- Efectuar un seguimiento efectivo al cumplimiento de las obligaciones del contratista/proveedor a través del supervisor del contrato/orden.
- Autorizar el pago del valor del contrato/orden de acuerdo con la forma establecida.
- Verificar el cumplimiento de las obligaciones del contratista frente al sistema General de Seguridad Social. Está obligación no será exigible si el contratista o proveedor es una persona jurídica o natural extranjera.
- Proporcionar toda la información que el contratista/proveedor requiera para el cumplimiento de sus actividades contractuales.
- Velar por el cumplimiento de las obligaciones del contrato/orden.

6.- VERIFICACIÓN DE LA INCLUSIÓN DE LA PRESENTE CONTRATACIÓN EN LOS ACUERDOS MARCO DE PRECIOS

El objeto de la presente contratación está en los Acuerdos Marco de Precios, pero por las razones técnicas presentadas en este estudio previo se adquirirá una solución por fuera de estos Acuerdos Marcos ya que se busca aumentar el nivel de seguridad digital de la Upme.

ANÁLISIS DE LOS EDR DISPONIBLES DEL ACUERDO MARCO DE PRECIOS

El cuadrante mágico de Gartner es una publicación que evalúa productos de tecnología en su eficiencia y efectividad, hace parte de esta evaluación los servicios de soporte y comercialización asociados a la empresa fabricante, es por ello por lo que Gartner se ha consolidado como un referente para las empresas

que contratan servicios y soluciones en TI ya que apoya la toma de las mejores decisiones en sus procesos de transformación digital.

Gartner es considerada la empresa mejor reputada en temas de consultoría y de investigación de las tecnologías de la información a nivel mundial por sus investigaciones, laboratorios y análisis sobre las herramientas y productos TIC más relevantes. Estar en el cuadrante garantiza la alta calidad de los servicios ofrecidos en materia tecnológica y un amplio conocimiento de las necesidades reales del mercado. Los líderes empresariales del mundo recurren a los análisis y estudios de Gartner en busca de guía y orientación, por ello es importante que en las herramientas de seguridad informática de la Unidad se cuente con un socio tecnológico de alta eficiencia pues el software malicioso es un tema transnacional que no conoce frontera y por ello las herramientas para afrontarlo deben ser las de mayor eficacia y eficiencia en los test de producto pero también en los esquemas de soporte y servicios conexos es importante tener un socio que brinde excelentes servicios y respaldos.

En ese sentido la Unidad de Planeación Minero-Energética - UPME hizo una apuesta por mejorar su seguridad informática buscando traer una solución **Endpoint de la más alta eficiencia y efectividad**, por ello se centró en los líderes de soluciones Endpoint del cuadrante de Gartner (Oct-2022) que en su última publicación vigente a mayo de 2023 presentaba como las soluciones de mayor eficiencia y efectividad en el mercado de EndPoint, a:

1. Microsoft Defender
2. CrowdSrtike
3. SentinelOne
4. Cyberseason
5. Trend Micro
6. Sophos

Con este panorama la Unidad revisó cuales de esas soluciones tienen distribución y soporte en Colombia encontrando que sólo hay representación de estas soluciones en el país para Microsoft, Trend Micro, Sophos. De la Solución SentinelOne se encontró sólo un distribuidor en Medellín.

Al revisar el Acuerdo Marco de Precios vigente para EDR se observan los siguientes: Defender, Sonic Wall, VMware Carbón Black EDR, G Data y Cisco Security Protection across Cloud & EndPoint, como se puede evidenciar, sólo Defender están entre los Endpoint de alta Eficiencia y Efectividad en la Seguridad Informática que brindan. Se da claridad que pese a estar relacionada en el Acuerdo Marco la solución de Endpoint ESET no está activa al 1 de junio de 2023 y no existe simulador aún para la adquisición de esta solución y sus servicios conexos. Así mismo se deja constancia que el día 2 de junio a las 10:30 am se evidencio que el producto ESET fue habilitado en el Acuerdo Marco de Precios y el simulador arrojo un valor de $113.192.090.50, pese a ello y una vez revisada la eficiencia técnica de esta solución se considera que no impacta la decisión recomendada, además porque no ofrece servicios de capacitación e instalación presencial y por las características técnicas de la infraestructura tecnológica de la entidad se requiere una implementación presencial para los servidores que no tienen salida a Internet, esto último implica la

configuración de un servidor de cache o agentes relay para la actualización de los endpoints y del cruce de información hacia la consola de administración.

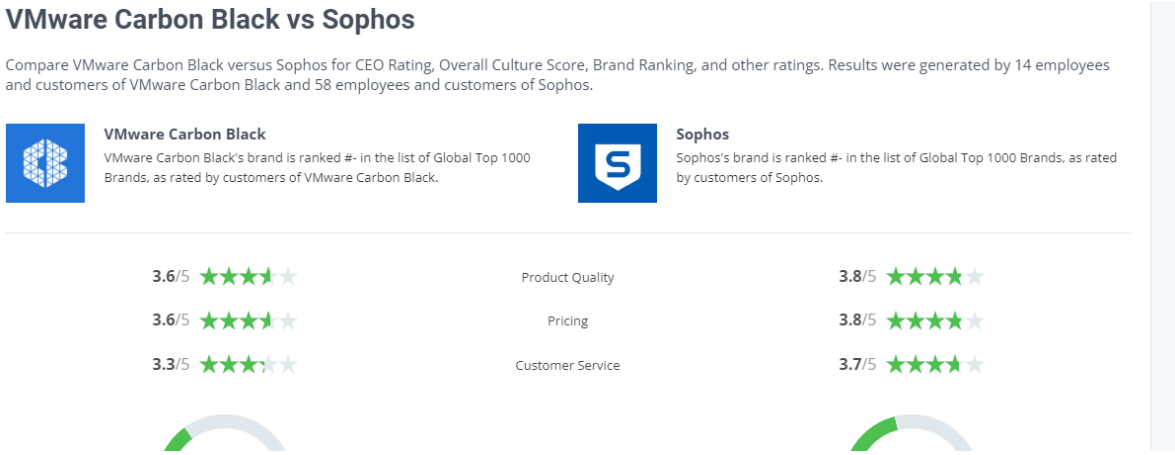
Así mismo se realizó un análisis exhaustivo de la soluciones disponibles para EDR del Acuerdo Marco presentando a continuación estos resultados:

GDATA En el acuerdo lo ofrecen como un Antivirus y se requiere un Endpoint su Costo es de $ 165.676.229.18 no cuenta con cortafuegos en el ENDPOINT. Un cortafuegos sirve para Permitir a los usuarios de la red interna utilicen recursos situados fuera de la red y para Impedir que los usuarios no autorizados de la red externa puedan utilizar los recursos de la red interna.

SONICWALL No cuenta con cortafuegos, análisis de malware deep learning (aprendizaje profundo) de menor desempeño, $ $183.401.556.45

VMWARE CARBON BLACK La gestión de políticas es engorrosa porque no tiene forma de aplicar las reglas a varios grupos. Si necesita configurar la misma regla para varias políticas, debe volver a escribirla. La actualización de agentes es lenta. En el simulador de CCE sólo está el ítem de capacitación para este EDR.

VMware Carbon Black Cloud	Sophos Intercept X Endpoint
View Product	View Product
Prioritization	Prioritization
Remediation Management	Remediation Management
Root Cause Analysis	Root Cause Analysis
Endpoint Protection	**Endpoint Protection**
Activity Log	Activity Log
Antivirus	Antivirus
Application Security	Application Security
Behavioral Analytics	Behavioral Analytics
Device Management	Device Management
Encryption	Encryption
Signature Matching	Signature Matching
Web Threat Management	Web Threat Management
Whitelisting / Blacklisting	Whitelisting / Blacklisting
IT Security	**Extended Detection and Response (XDR)**
Network Security	**Malware Removal**
Ransomware Protection	**Ransomware Protection**



CISCO SECURITY PROTECTION ACROSS CLOUD & ENDPOINT

Cisco Secure Endpoint viene en tres niveles: Essentials, Advantage y Premier, cada uno de los cuales agrega más EDR y capacidad de detección de amenazas. Secure Endpoint está integrado con los otros productos de seguridad de red e identidad de Cisco en Cisco SecureX. Cisco en el cuadrante de Gartner obtiene una buena puntuación en estrategia y ejecución de marketing, su éxito en este sentido se refleja en su fuerte cuota de mercado. Los puntajes de productos e innovación de Cisco se benefician de Cisco SecureX, una plataforma XDR que une las capacidades de seguridad de Cisco con capacidades de gestión de casos, búsqueda, investigación y remediación de productos cruzados. Cisco obtiene una buena puntuación por su estrategia de marketin, de distribución geográfica y sus extensos recursos de capacitación por las academias cisco, sin embargo, tiene grandes falencias como ausencia de un web control, Application control, control de dispositivos, entre otros.

A continuación, presentamos mayor detalle de los elementos preocupantes por su ausencia en esta solución de seguridad:

Cisco Secure Endpoint no proporciona un cortafuegos personal nativo ni ninguna capacidad de seguridad de datos, como ya se explicó.

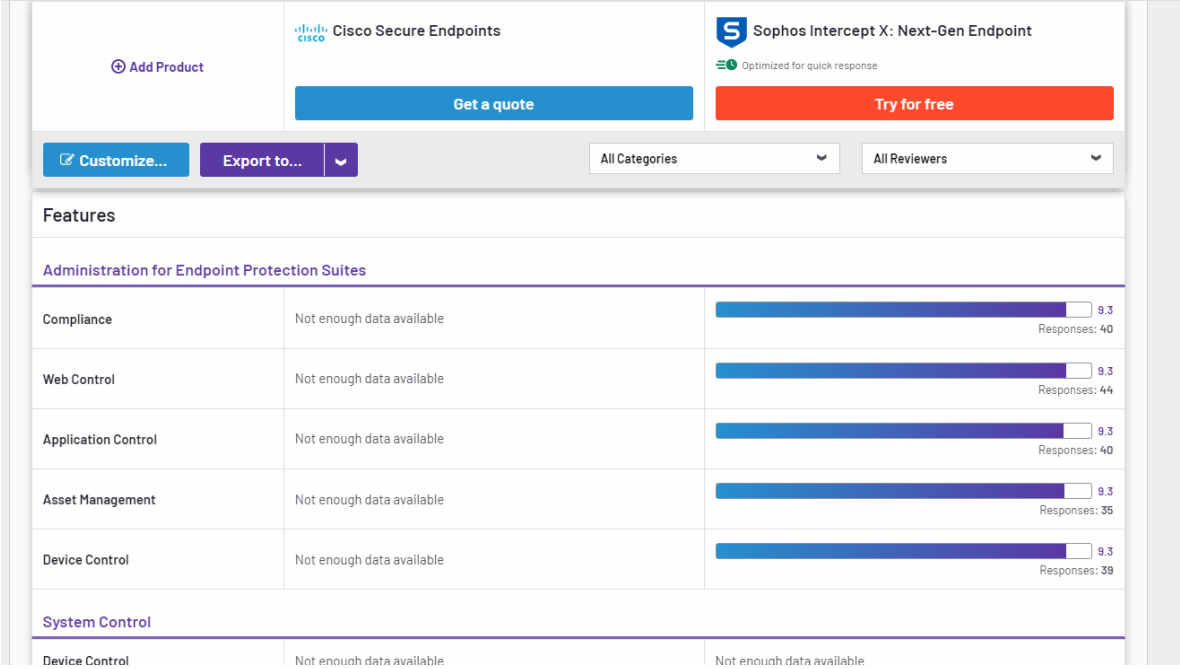
Cisco SecureX integra la cartera de productos EDR, Security Service Edge (SSE) y Secure Email Gateway (SEG) de Cisco para responder a incidentes, pero faltan consolas de administración e integración de políticas. Al no tener consolas de administración las labores de gestión y protección se dificultan, además es una diseñada para potenciarse al estar en un ecosistema cisco, ecosistemas más agnósticos no podrían recibir todo el potencial de la herramienta.

Las capacidades de remediación de EDR manual, como shell remoto, no están disponibles desde la consola SecureX. Buena parte de lo que se necesita de un EDR es esa respuesta automática o automatizada que en esta solución está bajamente implementada y por ello se habla de capacidades de remediación manual.

Cisco SecureX no almacena los datos de registro de forma centralizada, sino que obtiene datos a pedido de otros almacenes de registros. La función Orbital Advanced Search tiene una interfaz diferente de Cisco Secure Endpoint o SecureX

En el siguiente cuadro un comparativo de Cisco versus Sophos:

Caracteristicas	Cisco	Sophos
DESPLIEGUE		
Basado en web	cumple	cumple
De forma local LAN	cumple	cumple
COMPATIBILIDAD DISPOSITIVOS		
Escritorio	cumple	cumple
Movil	no cumple	cumple
Tableta	no cumple	cumple
Ipad	no cumple	cumple
SISTEMA OPERATIVO		
Linux	cumple	cumple
Windows	cumple	cumple
IOS	no cumple	cumple
Androide	no cumple	cumple
Mac OS	no cumple	cumple
FUNCIONES PRINCIPALES		
Controles de acceso/permisos	no cumple	no cumple
seguimiento actividad	cumple	cumple
Seguridad de la aplicación	cumple	cumple
Análisis de comportamientos	no cumple	cumple
Gestión de cumplimiento	no cumple	no cumple
Gestión de Dispositivos	cumple	cumple
cifrado	no cumple	cumple
Supervisión	no cumple	cumple
Escaneo de vulnerabilidades	no cumple	cumple
Gestión de amenazas Web	cumple	cumple



Ante este panorama la Unidad adelantó una revisión de todas las soluciones mencionadas en el Acuerdo Marco CCE-139-IAD-2020 pese a que algunas de ellas cuentan con documentación y referencias limitadas en internet se pudieron evidenciar faltantes técnicos importantes en estos EDR para una seguridad informática eficiente, como es el caso de las características no presentes de Application control, data 10os prevention, active adversary mitigations, protección contra robo de identidad, synchronized security heartbeat, Protección avanzada para servidores, Administración de certificados ssl, inteligencia de vulnerabilidad de aplicaciones, Integración de Capture Advanced Threat Protection (ATP) para probar automáticamente archivos sospechosos, Control del dispositivo, control de red, búsqueda de amenazas de visibilidad profunda y carcasa remota, entre otras. A lo dicho se suma el hecho de que en el acuerdo marco estos productos están atados a un solo proveedor lo cual está asociado a bajo conocimiento de la herramienta en el entorno local, pocos foros técnicos y hay un riesgo intrínseco en esta situación en sí mismo (poca literatura, pocos foros técnicos de esas soluciones y pocos sitios de respaldo de esas herramientas), por otra parte los costos económicos de implementación están en promedio en $150.000.000.oo lo que llevado a un análisis de costo eficiencia presenta un indicador fácilmente mejorable por otra solución en el mercado local. Por lo anterior y en atención al Artículo 42 del Manual de Contratación que permite no tener en cuenta los Acuerdo Marco de Precios en razón a las deficiencias técnicas que presentan los EDR allí ofertados o a los costos asociados a los mismos, la Oficina de Gestión de Información optó por no adquirir el servicio a través de Acuerdo Marco y procedió a hacer el estudio de mercado para hacer una contratación directa, por cuantía inferior a 150 smlmv, con mínimo 3 cotizaciones, como se explica en el acápite pertinente de estos estudios previos, con opciones de EDR que tengan gran representabilidad en Colombia y que estén con una alta eficiencia en el cuadrante de Gartner como lo son Microsoft, Trend Micro y Sophos.

En ese sentido la Unidad adelanto un estudio de mercado para adquirir una buena solución de seguridad EndPoint durante el mes de mayo de 2023, para ello revisó la última edición del cuadrante mágico de Gartner y en él se observó que los líderes para este tipo de soluciones son: Microsoft Defender, Trend Micro y Sophos, circunscribiéndonos a las soluciones líderes que tienen representación y soporte en Colombia. Teniendo conocimiento que la Solución de Microsoft podría adquirirse a través del acuerdo marco vigente se habló con el fabricante y se obtuvo un costeo de la solución cuyo costo estaba discriminado en $272.000.000 millones por valor del licenciamiento y $50.000.000 por valor de la implementación y con un tiempo asignado para esta actividad de aproximadamente dos meses. Así mismo se envió un anexo técnico y un formato de cotización a proveedores de las soluciones Trend Micro y Sophos.

Dentro del plazo establecido, 25 de mayo de 2023, para este estudio de mercado sólo se recibieron ofertas de proveedores de la solución Sophos Endpoint y de estas ofertas se recibieron 2 cotizando soluciones MDR, una cotizando una solución ENDPOINT y una cotizando una solución XDR. El día 29 de mayo llegaron 2 cotizaciones más una de Sophos y una de Tren Micro, ambas por valores muchísimo más elevados que las cuatro recibidas en el marco del estudio de mercado. Por tanto, se adjudicó el contrato a la empresa RTM quien ofreció una solución MDR que incluye el licenciamiento XDR y más el servicio de SOC 7x24, servicios de instalación y configuración, soporte, capacitación y 3 váucher para tomar una capacitación intensiva en la herramienta y poder certificarse en ella. A continuación se explica la diferencia entre los servicios ofertados:

Antivirus: Solución de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora. Brindan protección en tiempo real contra ataques de virus.

Endpoint: Herramienta de seguridad informática que brinda protección a través de sistemas antivirus y de algoritmos de inteligencia artificial para detectar posibles amenazas sobre los equipos finales de una red (servidores, portátiles y computadores).

XDR: Herramienta de seguridad informática conocida como un Endpoint extendido, tiene un alcance mayor al de un endpoint y de mayor profundidad en la detección de posibles amenazas sobre los equipos finales de una red (servidores, portátiles y computadores).

MDR: Servicio de seguridad informática conformado por un XDR y un SOC, entendido este último como un Centro de Operaciones Especializado de seguridad informática, en el SOC se cuenta con personal altamente especializado para monitoreo y correlación de eventos de seguridad sobre plataformas tecnológicas, advirtiendo de posibles amenazas con una alta fiabilidad.

7.- VERIFICACIÓN DE LA INCLUSIÓN DE LA PRESENTE CONTRATACIÓN EN EL PLAN ANUAL DE ADQUISICIONES

Los bienes y/o servicios a adquirir con la presente contratación se encuentran contemplados en el Plan Anual de Adquisiciones de la presente vigencia fiscal.

8. ANALISIS DE APLICACIÓN DE TRATADOS INTERNACIONALES DE LIBRE COMERCIO

De conformidad con la Guía para las Entidades Estatales con régimen especial de contratación, literal D, la Unidad de Planeación Minero-Energética – UPME debe verificar los acuerdos comerciales internacionales.

No obstante, teniendo en cuenta que el proceso de selección de la presente contratación es directa, no procede la verificación de aplicación de dichos acuerdos comerciales internacionales.

9.- IDENTIFICACIÓN DEL OBJETO EN EL CLASIFICADOR DE BIENES Y SERVICIOS

Se consultó el link **http://www.colombiacompra.gov.co/clasificador-de-bienes-y-servicios**, encontrando que el objeto de la presente contratación se encuentra clasificado así:

43233205 – Software de seguridad de transacciones y de protección contra virus

10.- NATURALEZA JURÍDICA DEL CONTRATO

La naturaleza jurídica del contrato a suscribir es de: compraventa

11.- MODALIDAD DE SELECCIÓN DEL CONTRATISTA

De conformidad con lo establecido en el artículo 39 de la Resolución UPME No. 184 del 24 de agosto de 2020 la modalidad de selección es DIRECTA, bajo la causal 39.3 "*Adquisición de bienes o servicios cuya cuantía sea igual o inferior a 150 SMMLV*".

12.- ANÁLISIS QUE SOPORTA EL VALOR ESTIMADO

Para determinar el valor estimado de la orden o contrato, la Unidad realizó el siguiente estudio del sector:

12.1.- Análisis de contrataciones similares en entidades Públicas

La Unidad de Planeación Minero-Energética – UPME consultó el link de Colombia Compra con el fin de identificar los valores de los contratos de los bienes o servicios similares al de la presente contratación, encontrando lo siguiente:

Entidad	Municipio de Sabaneta
Contrato	SAB-03-020-22
Objeto	RENOVACION DE LA PLATAFORMA DE GESTION UNIFICADA DE SEGURIDAD PERIMETRO Y ENDPOINT + XDR Y RENOVACIÓN DE LA SOLUCION DE RESPALDO PARA LOS SISTEMAS, MESA DE SERVICIOS Y MOTOR DE BASE DE DATOS PARA ELSISTEMA CORE DE LA ENTIDAD, QUE FORTALEZCAN LAS TIC EN LA ADMINISTRACIÓN MUNICIPAL
Costo	436.744.280 COP
Duración	1 Mes

Entidad	Imprenta Nacional de Colombia
Contrato	INC-058-202
Objeto	ACTUALIZACIÓN Y RENOVACIÓN DE LA PLATAFORMA DE SEGURIDAD INFORMÁTICA PERIMETRAL Y ENDPOINT DE LA IMPRENTA NACIONAL DE COLOMBIA

Costo	159.529.345 COP
Duración	12 Meses

Entidad	Alcaldía del Distrito Turístico y Cultural de Cartagena de Indias
Contrato	MC-DAAL023-2022
Objeto	CONTRATAR LA RENOVACIÓN, ACTUALIZACIÓN Y SOPORTE ESPECIALIZADO SOBRE EL LICENCIAMIENTO SOPHOS INTERCEPT XDR PARA LOS ENDPOINTS DE LA ALCALDÍA MAYOR DE CARTAGENA DE INDIAS POR EL TÉRMINO DE UN (1) AÑO
Costo	100.000.000 COP
Duración	25 Días

12.2.- Análisis de histórico de contrataciones de la entidad.

La Unidad de Planeación Minero-Energética – UPME consultó el histórico de contratación de la Entidad con el fin de identificar los valores de los contratos/ordenes de los bienes o servicios similares al de la presente contratación, encontrando lo siguiente:

Contrato	210-2016-120
Objeto	Renovación de las licencias para 170 usuarios de SYMC ENDPOINT PROTECTION ULTIMA VERSIÓN para la Unidad de Planeación Minero Energética.
Costo	$11.200.960
Duración	1 mes

Contrato	210-2017-145
Objeto	Renovar y adquirir licencias de Symantec Endpoint Protection para la Unidad de Planeación Minero Energética
Costo	$18.277.686
Duración	6 días hábiles

Contrato	O-032-2020
Objeto	Adquirir y licenciar una solución antivirus con EDR (Endpoint Detection Response), para la Unidad de Planeación Minero Energética - UPME
Costo	$49.238.889,71
Duración	3 años

Las soluciones de punto final han evolucionado en gran manera llevando el tema de antivirus a obsolescencia y por ello hoy se habla es de soluciones EDR y XDR que tienen inmerso un Antivirus pero son más que un Antivirus pues poseen un componente de Inteligencia Artificial que en la medida que tengan mayores capacidades de aprendizaje profundo son más efectivas técnicamente y por ende su costo es mayor, así mismo las soluciones que no evolucionaron y que son sólo antivirus son el nivel más bajo de protección pero así mismo de costos. El costo de los endpoint para los últimos 2 años ha incrementado más de 3 veces su valor debido a las necesidades que tienen las entidades y empresas de proteger su información, el activo más valioso que existe en la actualidad y que es aprovechado por los cibercriminales para realizar ataques como ransomware, spyware, malware y adware, por ende, ahora las empresas deben realizar una inversión mayor en ciberprotección, contar con software robusto y especializado que ayude a proteger su infraestructura tecnológica y sus datos.

Por lo anterior, la UPME considera importante invertir en un software robusto y especializado como lo es el MDR que cuenta con un gran valor agregado como es la solución especializada en seguridad informática SOC, el SOC integra gran apalancamiento tecnológico, procesos y personas capacitadas que ayudan a prevenir y proteger 7x24 su tecnología y datos de los cibercriminales, permitiendo detectar y responder ante ataques o amenazas en tiempo real. No en vano este tipo de soluciones son las mejor evaluadas por el consultor de tecnología mejor reputado del mundo: Cuadrante Mágico de Gartner, como se explicó anteriormente.

12.3.- Estudio de mercado

De conformidad con la causal de contratación directa, se realizó el siguiente sondeo de mercado

Para la adquisición de Microsoft Defender y se habló con ellos en su calidad de fabricante, nos aclararon que por el Acuerdo Marco de Precios podríamos adquirir el Endpoint y que de los dos planes que están allí se debe seleccionar el Plan 2, así mismo nos indicaron que se debían adquirir otros componente de software para poder implementar esta solución y nos ayudaron a diligenciar el simulador, dándonos unos costos de licenciamiento por valor de **$274.344.000.00**, así mismo nos referenció uno de sus Partner para cotizar los servicios de instalación, configuración y puesta en producción del Endpoint, los costos de estos servicios fueron de **$56.510.125.00**, esta implementación tomaría unas 180 horas luego de firmado el contrato y los tiempos del Acuerdo Marco para contratación son más o menos de 34 días, según lo expresado por ellos mismos.

Dado que el presupuesto asignado para esta contratación era inferior a la propuesta de Microsoft, la Unidad procedió a hacer un anexo técnico, con las necesidades de la UPME para garantizar que se consideraran los mínimos técnicos para una nueva solución EDR a contratar, además este anexo técnico había sido presentado por el Especialista de Seguridad Informática de la UPME, una vez ajustado, se envió el Anexo Técnico y formato de cotización a todos los partner registrados en Internet, para Colombia, de las siguientes soluciones Endpoint: Trend Micro, Sophos y SentinelOne y se dio el día 25 de mayo como fecha límite para cotizar. Dentro del tiempo establecido para el estudio de mercado se recibieron 4 propuestas que ofertaron EDR, XDR y MDR todos de la solución SOPHOS. El día de ayer 30 de mayo se recibió un email de la solución SentinelOne presentando la solución y poniéndose a la orden de la Unidad, pero no hubo cotización, así mismo llegó un email por parte de un proveedor de la solución EndPoint de Trend Micro cuyos costos totales corresponden a:

SOLUCIÓN/SERVICIO	CANTIDAD	VALOR TOTAL (12 MESES)	VALOR TOTAL (36 MESES)
Solución para endpoint - Apex One as a Service includes Mac, iDLP, iVP and iAC Normal Users New - por año	200	$ 34.347.275,72	$ 99.140.416,15
Solución para servidores- Trend Micro Cloud One - Workload Security with XDR Normal Devices New - Por año	150	$ 315.119.302,91	$ 909.564.388,29
Solución para protección de buzones correo - Cloud App Security Advanced - Por año	300	$ 105.795.971,37	$ 305.370.845,56
	SUBTOTAL	$ 455.262.550,00	$ 1.314.075.650,00
	IVA	$ 86.499.884,50	$ 249.674.373,50
	TOTAL	$ 541.762.434,50	$ 1.563.750.023,50

Por lo anterior, la Oficina de gestión de la información adelantó el estudio de mercado mediante invitación vía correo electrónico a las empresas referidas por el fabricante de la solución Sophos: INSITEL radicado

UPME 20231110093572, RTM radicado UPME 20231110091822, SKILLNET radicado UPME 20231110091832 y SODITEK radicado UPME 20231110091852.

A continuación, se detallan los costos ofertados para esta contratación y que están dentro los márgenes previstos para la misma:

Nombre del Proveedor		SKILLNET		SODITEK		RTM		INSITEL	
PRODUCTO OFERTADO		MDR SOPHOS		XDR SOPHOS		MDR SOPHOS		EDR SOPHOS	
PRODUCTO	CANTIDAD	VR UNITARIO	VR TOTAL CON IVA	VR UNITARIO	VR TOTAL CON IVA	VR UNITARIO	VR TOTAL CON IVA	VR UNITARIO	VR TOTAL CON IVA
Adquisición de un Endpoint Antivirus con EDR (Endpoint Detection Response)	350	USD 30.024	$141,113,150,00	$451,146,78	$ 157,901,373,00	$358,045,33	$ 125,315,865,00	$218,085,71	$ 76,330,000,00
Garantía de fabricante sobre los productos adquiridos por un año	1	$ -	$ -	$ -	$ -	$ -	$ -	$ 31,472,900,00	$ 31,472,900,00
Soporte local sobre los productos adquiridos por un año de lunes a sabado de 7 am a 7 pm	1	$ 15,000,000,00	$ 15,000,001,00	$ -	$ -	$ -	$ -	$ 19,231,100,00	$ 22,885,009,00
Transferencia de conocimiento sobre el manejo y administración de las soluciones adquiridas de mínimo 16 horas (1 Paquete).	1	$ 117,800,000,00	$ 117,800,001,00	$ 1,900,000,00	$ 2,261,000,00	$ -	$ -	$ 8,930,300,00	$ 10,627,057,00
Servicios de instalación, configuración, puesta en funcionamiento a total satisfacción de la entidad.	1			$ 19,000,000,00	$ 22,610,000,00	$ 13,428,511,00	$ 15,979,928,00	$ 5,554,900,00	$ 6,610,331,00
			$273,913,152,00		$182,772,373,00		**$141,295,793,00**		$147,925,297,00

De los valores presentados por los proponentes se selecciona RTM ya que representa la mejor propuesta de solución con un MDR Complete que cuenta con un servicio de monitoreo 24x7 de caza y respuesta ante amenazas (SOC) por un valor de $141.295.793.

Con el estudio de mercado construido y la evaluación técnica, el panorama de la Unidad era que teníamos dos ofrecimientos de los productos Endpoint de mayor seguridad de la solución Sophos: Un MDR. De los dos ofrecimientos la oferta de menor valor es la de la empresa **RTM** cuyo costo es de **$141.295.793.** Por tanto, la Of. De Gestión de la Información recomienda hacer dicha adquisición, ya que dotará a la Unidad de Planeación Minero-Energética de una herramienta de alta eficiencia y efectividad en la prestación de la seguridad informática de la entidad, lo que a su vez es un mayor resguardo para la seguridad de la Información de la entidad y un riesgo menor de ser atacados por software malicioso.

Para hacer el análisis técnico de las ofertas presentadas se contó con el consenso de 4 ingenieros de la Oficina de Gestión de la Información, así: Ing. Alexander Pérez, Ing. Miguel Barrera, Ing. Claudia Beltrán e Ing. John Barrios quienes recomendaron contratar la solución ofertada por la empresa RTM por considerarla el mejor producto y además la oferta de RTM tiene la de mejor relación costo/eficiencia, así mismo la jefe de la Oficina Ing. Olga Lucía Morales y especialista en seguridad informática avaló la evaluación realizada.

Conclusión

De lo anterior se concluye que el valor para la presente contratación se encuentra ajustado al Mercado y, es coherente con lo que la Entidad y/u otras, ha pagado por servicios o bienes similares en años anteriores, con los correspondientes incrementos de ley.

13.- JUSTIFICACIÓN DE LOS FACTORES TÉCNICOS DE SELECCIÓN QUE PERMITEN IDENTIFICAR LA OFERTA MÁS FAVORABLE

El factor de selección que permitió identificar la oferta de RTM como la más favorable, fue: menor precio

por la misma solución, ya que ofrece un MDR complete de Sophos, es decir, brinda una tecnología completa de endpoint que reúne el endpoint extendido (XDR) y un servicio especializado de analistas e ingenieros de seguridad que monitorean 24x7 las amenazas, este servicio especializado es denominado (SOC) el cual logra realizar un análisis profundo y avanzado de las actividades que se realizan en redes, servidores, terminales, bases de datos, aplicaciones, sitios web e infraestructura.

Por otro lado, el proveedor brinda un voucher para tres profesionales que puedan certificarse como administrador de Sophos Central en Bogotá.

14. PRESUPUESTO ASIGNADO Y VALOR MÁXIMO DEL CONTRATO:

De conformidad con lo precedido, el presupuesto asignado para esta contratación es de $ 141.295.793 (Ciento cuarenta y un millones doscientos noventa y cinco mil setecientos noventa y tres pesos), que se pagará con cargo al:

Rubro: C-2199-1900-5-0-2199067-02 Fortalecimiento de los servicios digitales aumentando la capacidad para la transformación digital e interacción con el ciudadano Nacional
Recurso: 20 Ingresos Corrientes
Del presupuesto de: Inversión

Este valor incluye todos los costos asociados, directos e indirectos, IVA sí hay lugar, retención en la fuente y cualquier otro costo o impuesto en que se incurra el contratista para la ejecución de la presente orden o contrato.

15. FORMA DE PAGO

El valor del contrato/orden se pagara en 1 pago, previa radicación de la cuenta de cobro o factura electrónica correspondiente, si hay lugar, acompañada del certificado del pago de los aportes a la Seguridad Social Integral y Parafiscales, expedida por el Representante Legal o el Revisor Fiscal, según sea el caso, junto con la presentación de los informes y el certificado de cumplimiento expedido por el supervisor de la orden o contrato, donde coste el ingreso a almacén, cuando haya lugar, así:

Número de pago	Porcentaje del valor	Momento del pago	Contra que se paga
Uno	**100%**	Luego del primer mes de ejecución del contrato	Entrega a satisfacción de la Entidad de las obligaciones específicas, productos y servicios.

16. PLAZO ESTIMADO DE LA EJECUCION DEL CONTRATO:

El plazo de ejecución será de treinta (30) días calendario contados a partir del día de la expedición del registro presupuestal o aprobación de garantía, si hay lugar a solicitarla.

El plazo de la vigencia del licenciamiento y soporte contratado será por el término de un (1) año, contado a partir de la suscripción.

17. ESTIMACIÓN, TIPIFICACIÓN Y ASIGNACIÓN DE RIESGOS PREVISIBLES INVOLUCRADOS EN LA PRESENTE CONTRATACIÓN Y DESARROLLO DEL PROCESO.

Los riesgos que puedan afectar el equilibrio económico del contrato a celebrar se estiman, tipifican y asignan de acuerdo con el Formato de tipificación, estimación y asignación de riesgos, de conformidad con la siguiente tabla.

No.	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	General	Interno	Pre Contratación	Operacional	**Retraso en la consecución de documentos o en la firma del contrato**	**Retraso en la ejecución del contrato**	2	3	5	Medio	Contratista	Requerimientos y ajuste del cronograma de ejecución	1	2	3	Bajo	Si	Grupo de contratación	**Desde la adjudicación o selección**	**Mediante requerimientos, correos electrónicos**	Inmediatamente	Diaria
2	General	Interno	Pre Contratación	Operacional	**Retraso en la presentación de las garantías.**	**Retraso en la ejecución del contrato**	2	3	5	Medio	Contratista	Requerimientos y ajuste del cronograma de ejecución	1	2	3	Bajo	Si	Grupo de contratación	**Desde la adjudicación o selección**	**Mediante requerimientos, correos electrónicos**	Inmediatamente	Diaria
3	Específico	Externo	Ejecución	Operacional	**Demora en la prestación del servicio**	**Retraso en la ejecución del contrato**	3	3	6	Alto	Contratista	Efectuar seguimiento permanente por parte del supervisor del contrato para que se un adecuado cumplimiento al objeto del contrato	2	3	5	Medio	Si	Contratista Entidad	**Desde el inicio del contrato/orden**	**Mediante informes.**	Cuando ocurra	Diario
4	General	Interno	Ejecución	Operacional	**Daño o perdida de bienes de la entidad imputables al contratista durante la ejecución al contrato**	**Demora en las labores diarias de funcionarios y/o contratistas de la entidad.** **Detrimentopatrimonial dela UPME**	2	3	5	Medio	Contratista	Llevar a cabo inspecciones preventivas permanentes Registro de traslados de bienes	1	2	3	Bajo	Si	Contratista Entidad	**Desde el inicio del contrato/orden y hasta su finalización**	**Inspecciones preventivas permanentes**	Diarias	Diaria
5	Específico	Externo	Ejecución	Operacional	**Que se presenten accidentes de trabajo del contratista o del personal de contratista, sufridos al momento de prestarle el servicio dentro de las instalaciones de la Entidad**	**Demora en las labores diarias de la entidad y por ende a los usuarios finales**	2	2	4	Bajo	Contratista	Que se reemplace la persona por una igual de idónea para ejecutar la labor. El contratista deberá dar notificación a su ARL	2	1	3	Bajo	Si	Contratista	**Desde el comienzo de la ejecución del contrato, firma acta de inicio**	**Mediante informes y certificado de cumplimiento a satisfacción**	Cuando ocurra	Cuando ocurra

No.	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
6	Específico	Externo	Ejecución	Operacional	**No contar con el personal certificado y calificado para la prestación del servicio**	**Poner en riesgo a la entidad debido a que no se cuente con el personal calificado para el desarrollo del contrato.**	3	2	5	Medio	Contratista	Efectuar seguimiento permanente por parte del supervisor del contrato Demostrar la idoneidad de la persona Garantías	2	2	4	Bajo	Si	Contratista	Desde la firma del acta de inicio	Mediante informes y certificado o de cumplimiento a satisfacción	Cuando ocurra.	Cuando ocurra
7	Específico	Externo	Ejecución	Operacional	**No pago de las obligaciones a proveedores, salarios y seguridad social del personal a cargo**	**Demora en las labores diarias y misionales de la entidad y por consecuencia a él o los usuarios finales.** **Incumplimiento contractual**	2	2	4	Bajo	Contratista	Garantías No efectuar el pago hasta que no cumpla con los requisitos exigidos por la normatividad.	2	1	3	Bajo	Si	Supervisor del contrato	Desde el comienzo de la ejecución del contrato	Mediante informes y certificado o de cumplimiento a satisfacción	Cuando ocurra.	Cuando ocurra

18. GARANTÍAS.

No es necesario constituir garantías, dada la naturaleza del contrato, su objeto y su forma de pago.

19. LUGAR DE EJECUCIÓN

El desarrollo del contrato/orden será en la ciudad de Bogotá D.C.

20. SUPERVISIÓN

La supervisión del contrato/orden será ejercida por: Claudia Marcela Beltrán Profesional Especializado Grado 15

21. DOCUMENTOS ANEXOS

a. CDP.
b. Cotizaciones del estudio de mercado

Dependencia	Oficina de Gestión de la Información
Elaboró	John Alejandro Barrios Ávila
Aprobó	Olga Lucía Morales Nova