ANEXO. ESTUDIO DE SECTOR
ESTUDIOS PREVIOS DE CONTRATACIÓN DIRECTA

Adquirir el servicio de ciberseguridad contra ransomware y el licenciamiento de la solución Endpoint con la que cuenta la UPME.

NOVIEMBRE 2025

1. OBJETIVO DEL ESTUDIO

Adquirir el servicio de ciberseguridad contra ransomware y el licenciamiento de la solución Endpoint con la que cuenta la UPME.

2. ANÁLISIS DEL SECTOR

1.1. ASPECTOS GENERALES

Necesidad del servicio:

El Decreto 2121 del 11 de diciembre de 2023 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.

La UPME tiene como objeto planear en forma integral, indicativa, permanente y coordinada con los agentes del sector minero energético, el desarrollo y aprovechamiento de los recursos mineros y energéticos; producir y divulgar la información requerida para la formulación de política y toma de decisiones; y apoyar al Ministerio de Minas y Energía en el logro de sus objetivos y metas.

De conformidad con lo definido en el artículo 12 ibidem, es responsabilidad de la Oficina de Tecnologías de la Información – OTI de la UPME: *"4. Implementar los lineamientos de política y estándares relacionados con el diseño y desarrollo de infraestructura tecnológica y servicios de TI, la interoperabilidad de sistemas de información, marco de referencia de arquitectura empresarial, el modelo de seguridad y privacidad de la información y la prestación de los servicios ciudadanos digitales, de acuerdo con la misionalidad de la entidad (...)*, entre otras funciones.

El Decreto 1008 de 2018, establece los lineamientos generales de la Política de Gobierno Digital para Colombia, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

A través del Decreto 767 de 2022 se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones'; así mismo, mediante la Resolución 500 de 2021,

expedida por el MinTIC, se establecieron los lineamientos y estándares para la estrategia de seguridad digital, y la adopción del modelo de seguridad y privacidad, como habilitador de la política de Gobierno Digital.

Con el fin de dar cumplimiento a los objetivos de la OTI y los Planes formulados, alineados al MIPG, de formuló el proyecto de inversión: "Fortalecimiento de los servicios digitales aumentando la capacidad para la transformación digital e interacción con el ciudadano", el cual busca fortalecer la apropiación de los productos y servicios por parte de la Ciudadanía y Actores clave de la Entidad, por medio del fortalecimiento de la gestión de capacidades de TI que permitan la satisfacción de los grupos de interés y ciudadanía en general, a través de la estrategia y gestión de TI. De este modo, se busca alcanzar la modernización de la arquitectura tecnológica y de aplicaciones, alineándose con la identificación de las soluciones existentes en el mercado que respondan a las necesidades institucionales, enmarcadas en tecnologías amigables con el medio ambiente y, en línea con lo establecido en el ejercicio de arquitectura empresarial que corresponde a la lógica de los procesos de negocio y la infraestructura de TI que reflejan los requisitos de integración y normalización del modelo de funcionamiento de la Unidad.

El proyecto anteriormente relacionado, se plantea como uno de sus objetivos Incrementar el desarrollo de los habilitadores transversales de la política de gobierno digital y la actividad de Definir y estructurar las acciones tendientes a la apropiación e implementación de la política de Gobierno Digital, a través de la cual se busca la: Revisión y actualización del Modelo de Seguridad y Privacidad de la Información; la definición de la estrategia para uso, apropiación, y la gestión del cambio; el ejercicio de Arquitectura Empresarial para la identificación y desarrollo de proyectos que articulen la visión de negocio con las soluciones de TI; la revisión y actualización del PETI; Formular y ejecutar Plan de Continuidad de TI.

Para dar cumplimiento a lo anterior, la UPME formuló el Plan Estratégico de Tecnologías de la Información, el cual se propone implementar la estrategia de arquitectura empresarial, entendida como una práctica estratégica que permite analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de evaluar y diagnosticar su estado actual y establecer la transformación digital necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad.

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 denegación 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 técnicas. 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.

Considerando 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 Sistema de Gestión de Seguridad de la Información -SGSI- y por tanto es importante contar con plataforma tecnológica para la protección de la información y de la plataforma tecnológica de la Unidad, razón por la que resulta necesario contar con una solución de Endpoint (computadores, portátiles, tabletas, etc) como primera línea de defensa del ecosistema digital de la UPME.

Aspecto regulatorio:

- Ley 1581 de 2012 - Régimen General de Protección de Datos Personales: Establece normas para la protección de datos personales en Colombia, aplicable a cualquier sistema de información que almacene o procese datos personales.
- Decreto 1078 de 2015 - Decreto Único del Sector TIC: Contiene disposiciones relacionadas con la seguridad digital en las entidades públicas.3
- Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC: Define directrices para la protección de la infraestructura tecnológica en entidades públicas.
- ISO 27001:2022 - Norma Internacional sobre Seguridad de la Información: Referente para la gestión de riesgos y la implementación de controles de seguridad en sistemas de información.
  Ley 1341 de 2009 - Principios y regulación de las TIC en Colombia: Establece principios para la gestión de tecnologías de información y telecomunicaciones en el país.

Requerimientos, especificaciones, condiciones (tiempo de entrega) o descripción del servicio requerido:

- Suministrar 310 licencias de la solución tipo MDR Complete de Sophos (Licenciamiento XDR + SOC) para protección antimalware de computadores (180), servidores (130) por 12 meses.
- Suministrar el soporte extendido para sistemas operativos que están saliendo del ciclo de vida de soporte.
- Prestar servicio gestionado de ciberseguridad a través del Centro de Operaciones de Seguridad del proveedor, con alcance en todas las soluciones específicas de seguridad con las que cuenta la UPME y que se integran con el MDR Complete de Sophos, para realizar el análisis, detección y respuesta a ciberataques dirigidos contra equipos, servidores, redes, cuentas de correo electrónico, entre otros elementos o servicios de la infraestructura de TI.
- Prestar servicio de monitoreo 24x7 de caza y respuesta ante amenazas (SOC) para la plataforma tecnológica de la Unidad, con el alcance y características presentadas en la oferta.
- Cumplir con las especificaciones técnicas establecidas en la oferta.
- Brindar la operación las 24 horas del día, los 7 días de la semana, para garantizar un monitoreo constante de la plataforma tecnológica de la Unidad. Esto implica la supervisión en tiempo real de registros de eventos, alertas de seguridad y otras fuentes de datos relevantes, de acuerdo con el alcance y características presentadas en la oferta.
- Prestar el soporte técnico sobre la solución que permita: prevenir, detectar y neutralizar software malicioso en la infraestructura de la Entidad, por el término del presente proceso.
- Garantizar que la solución se integra y puede interoperar con soluciones específicas de seguridad con las que cuenta la Entidad y que generan la telemetría insumo para el SOC con el fin de realizar la gestión de amenazas de ciberseguridad.
- Contar con la integración con diferentes framework (MITRE ATT&CK) con el fin de contar con una clasificación de los eventos, las técnicas y tácticas utilizadas por los atacantes a nivel mundial.
- Adoptar medidas inmediatas para mitigar el impacto, en caso de que se confirme una amenaza o incidente de seguridad. Esto podría incluir el aislamiento de sistemas comprometidos, la eliminación de malware y la implementación de medidas de seguridad adicionales.
- Brindar el servicio de protección, detección y respuesta a incidentes de seguridad 24/7 totalmente gestionado por el servicio de MDR complete, que proporcionará el soporte telefónico directo, la asignación de un responsable de respuesta a incidentes dedicado, garantizando que las amenazas se eliminen por completo.

- Realizar la investigación de la causa raíz de los incidentes para ayudar a prevenir ataques futuros.
- Atender los acuerdos de niveles de servicio establecidos con el supervisor del contrato asignado por la UPME.
- Garantizar que la plataforma cuenta con reportes predefinidos y personalizados que permitan visualizar los eventos de forma eficiente y tomar decisiones en torno a éstos.
- Realizar la gestión, monitoreo, correlación de eventos y resolución de eventos e incidentes de seguridad, sobre la infraestructura tecnológica de la UPME, objeto del contrato.
- Realizar transferencia de conocimiento sobre la herramienta o solución a los profesionales designados por el supervisor del contrato, con el fin de que estén en la capacidad de realizar modificaciones en caso de requerirse.
- Contar con la capacidad de identificar y analizar amenazas cibernéticas como intrusiones, malware, intentos de acceso no autorizados y otras actividades anómalas sobre la plataforma tecnológica de la Entidad.
- Establecer una comunicación efectiva con la UPME y otras partes interesadas, a través del supervisor del contrato. Esto implica la colaboración en la planificación de estrategias de seguridad, la coordinación de actividades de respuesta a incidentes y la transmisión de información relevante.
- Cumplir con las regulaciones y estándares de seguridad aplicables a la industria y a la ubicación geográfica donde la UPME desarrolla las actividades.
- Contar con la configuración de reglas, alertas y notificaciones preconfiguradas y parametrizables aplicables a los activos monitoreados. Las alertas mínimas para monitorear son:
    - Actividades asociadas a la administración de cuentas de usuario final
    - Cambios de parámetros técnicos, de configuración o de seguridad.
    - Cambios de configuración horaria.
    - Actividades de conexión con cuentas de usuario final o administradores.
    - Actividades asociadas a los logs de la plataforma de correlación.
    - Actividades asociadas a conexión de acceso remoto (RDP).
    - Ataques de fuerza bruta.
    - Múltiples login fallidos desde una misma estación de trabajo.
    - Cuentas de Windows creadas y eliminadas
    - Malware o programas potencialmente no deseados detectados.
    - Ataques DoS (Denial of Services attack) y DDoS (Distributed Denial of Services Attack).
    - También las sugeridas por las buenas prácticas de monitoreo de infraestructuras tecnológicas.
- Contar con las actualizaciones permanentes que libere el fabricante de la solución adquirida.
- Mantener la certificación de distribuidor gold partner.

- Entrega a satisfacción de la Unidad de Planeación Minero-Energética de los productos y servicios prestados.

Productos:

No de licencias	Producto	Periodo
180	Central Managed Detection and Response Complete - 200-499 users - 12 MOS - Renovación	Nov 6 2025 a Nov 5 2026
130	Central Managed Detection and Response Complete Server - 100-999 servers - 12 MOS - Renovación	Nov 6 2025 a Nov 5 2026
1	Central Extended Support for W7/8.1/2008 R2/2012/2012 R2 - 1-499 users - 12 MOS - Renovación	Nov 6 2025 a Nov 5 2026

1. Informe mensual del servicio SOC
2. Certificación de Licenciamiento adquirido por la UPME indicando el derecho a soporte durante la vigencia del licenciamiento y certificación del servicio SOC.

Entrega de bienes

El contratista deberá entregar el siguiente bien intangible: certificado de licenciamiento el cual se deberá ingresar al almacén, donde se indique la vigencia de las licencias.

Clasificador de Bienes y Servicios UNSPSC:

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:

Código UNSPSC 43233204 Producto: Software de seguridad y de protección contra virus.

Deber de análisis de las Entidades estatales:
La entidad realizó un análisis de procesos en el portal SECOP II con especificaciones técnicas similares al objeto del presente proceso, con el objetivo de conocer la dinámica del mercado, incluyendo presupuesto y modalidad de selección, este análisis permitió identificar actores clave, evaluar la competencia y evaluar el presupuesto según la oferta disponible, también se revisaron términos de pago y condiciones contractuales previas para asegurar su viabilidad, adicionalmente, desde una perspectiva técnica, se compararon especificaciones para garantizar calidad y cumplimiento, mientras que se evaluaron riesgos potenciales y se establecieron medidas de mitigación para asegurar una ejecución eficiente.

Sustentación del porqué se requiere hacer una contratación directa:
De conformidad con lo establecido en el capítulo 2 del artículo 47 del Manual de Contratación adoptado por la Resolución UPME 026 de 2025, la modalidad de selección es DIRECTA, bajo la causal de: "47.4. Contratos cuya cuantía sea igual o inferior a 150 SMMLV.".

Análisis del valor del Presupuesto:
Se procedió desde la Oficina de Tecnologías de la Información a realizar un análisis a través de la solicitud de información a diferentes actores del mercado que cuentan con la capacidad de proveer este producto y con el propósito de identificar el valor adecuado del presupuesto para la adquisición de 310 licencias de la solución tipo MDR Complete de Sophos (Licenciamiento XDR + SOC) para protección antimalware de computadores (180), servidores (130) por 12 meses, para ello se realizó un sondeo de mercado que nos permitiera identificar las empresas que cumplieran las características técnicas requeridas por la Entidad, y a su vez establecer un monto acorde a las tarifas del mercado; como resultado de este ejercicio se estableció que el valor más adecuado para este proceso corresponde a **CIENTO TREINTA Y SIETE MILLONES CUATROCIENTOS NOVENTA MIL PESOS ($137.490.000) M/CTE** cumpliendo con las características técnicas exigidas y el cual se adapta a las dinámicas mercantiles al no encontrar diferencias significativas, este fue el menor valor ofertado y lo presentó la empresa **Redes Tercer Milenio**.

En el título 2. Histórico de la Contratación se realiza un análisis detallado de la información obtenida en el mercado, en la que además se consideraron históricos de la contratación de la Unidad de Planeación Minero Energética – UPME y de otras entidades estatales, dentro de las variables consideradas para la fijación del presupuesto se encuentra el cubrimiento de los requerimientos técnicos específicos con los que debe contar la certificación para satisfacer la necesidad institucional y el valor indicado por los diferentes proveedores consultados, demostrando que el presupuesto asignado es adecuado y coherente con el bien exigido en la presente contratación.

2. HISTÓRICO DE CONTRATACIÓN

Por parte de la UPME:
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 de los bienes o servicios similares al de la presente contratación, encontrando lo siguiente:

CONTRATO	CO1.PCCNTR.5037675
OBJETO	Adquirir una solución Endpoint antivirus para la UPME

COSTO	$141.295.793
MODALIDAD	DIRECTA
DURACIÓN	1 año

CONTRATO	CO1.PCCNTR.5460122
OBJETO	Contratar los servicios de un Centro de Operaciones de Seguridad SOC para realizar la gestión y el monitoreo de la infraestructura tecnológica y la gestión de eventos e incidentes de seguridad.
COSTO	$147.740.900
MODALIDAD	DIRECTA
DURACIÓN	1 año

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
MODALIDAD	DIRECTA
DURACIÓN	3 años

Por parte de otras Entidades:

La Unidad de Planeación Minero Energética – UPME consultó la página web 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	Personería de Bogotá
CONTRATO	PB-SASI-2004-0002
OBJETO	RENOVACIÓN DE LAS LICENCIAS ANTIVIRUS PARA LA PERSONERÍA DE BOGOTÁ D.C
COSTO	$340.000.000COP
MODALIDAD	Directa
DURACIÓN	12 meses

ENTIDAD	Municipio de la Ceja
CONTRATO	2024.10.05.05.041.311
OBJETO	RENOVACIÓN DE LICENCIAS DE SOFTWARE (ANTIVIRUS) PARA LAS DEPENDENCIAS DE LA ADMINISTRACIÓN MUNICIPAL
COSTO	$ 36.400.000 COP
MODALIDAD	Directa
DURACIÓN	12 Meses

ENTIDAD	MUNICIPIO DE PITALITO
CONTRATO	MP-SG-MC-CV-006-2024
OBJETO	RENOVACIÓN DE LICENCIAMIENTO DE ANTIVIRUS CENTRAL INTERCEPT X ADVANCED PARA ENDPOINT Y SERVIDORES, PARA LOS EQUIPOS DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MUNICIPIO DE PITALITO
COSTO	$ 58.500.000 COP
MODALIDAD	Directa
DURACIÓN	12 meses

3. ESTUDIO DEL MERCADO

El estudio de mercado comprende el análisis de los precios con el fin de establecer el presupuesto oficial del proceso de contratación y de conformidad con la causal de contratación directa, se realizó el siguiente sondeo de mercado:

La Oficina de Tecnología de la Información adelantó el estudio de mercado solicitando cotización a tres (3) empresas (SODITEK; RTM; SKY SYSTEM), las mismas se encuentran en un listado de posibles proveedores con que cuenta la OTI según el objeto del contrato, de las cuales se realizó un análisis de precios:

DESCRIPCIÓN	CANT	SODITEK	RTM	SKY SYSTEM
Central Managed Detection and Response Complete - 200-499 users - 12 MOS - Renewal - GOV	180	$ 88.281.180	$ 70.624.980	$ 89.901.180
Central Managed Detection and Response Complete Server - 100-999 servers - 12 MOS - Renewal - GOV	130	$ 69.370.990	$ 55.496.870	$ 70.956.990
Central Extended Support for W7/8.1/2008 R2/2012/2012 R2 - 1-499 users - 12 MOS - Renewal	1	$ 14.210.187	$ 11.368.150	$ 15.780.187
	TOTAL	$ 171.862.357	$ 137.490.000	$ 176.638.357

De acuerdo con lo anterior, se toma como base del presupuesto la menor propuesta, de las cotizaciones del sondeo de mercado recibidas, correspondiente a **CIENTO TREINTA Y SIETE MILLONES CUATROCIENTOS NOVENTA MIL PESOS (137.490.000) M/CTE**

En el marco del proceso de contratación directa, se procedió a seleccionar al proveedor que presentó la oferta de menor valor, toda vez que la totalidad de los proponentes cotizaron los mismos servicios bajo condiciones equivalentes, la decisión se sustenta en que, al tratarse de propuestas comparables en términos de calidad, alcance y especificaciones técnicas, el precio se constituye en el criterio determinante, garantizando con ello la optimización de los recursos financieros de la Entidad y el cumplimiento de los principios de eficiencia, eficacia y economía que rigen la contratación pública.

De igual manera, se llevó a cabo la verificación de la experiencia del proveedor, con el propósito de asegurar la capacidad para el cumplimiento del objeto contractual, confirmando que se trata de la opción más conveniente para la Entidad.

CONCLUSIÓN

El factor de selección que permitió identificar la oferta de **Redes Tercer Milenio** como la más favorable de conformidad con el estudio de sector elaborado, fue:

1. **Menor Precio:**

    - **Análisis de Costos:** Se realizó un análisis comparativo de los costos de las diferentes propuestas recibidas. La oferta de **Redes Tercer Milenio** presentó el precio más bajo en relación con los servicios ofertados, lo cual representa un ahorro significativo para la entidad sin comprometer la calidad.
    - **Presupuesto:** La oferta se ajusta al presupuesto asignado para este proyecto, permitiendo una asignación eficiente de los recursos financieros.

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.

4. ANEXOS

1. Cotizaciones