ANEXO. ESTUDIO DE SECTOR
ESTUDIOS PREVIOS DE CONTRATACIÓN DIRECTA

Adquirir el licenciamiento de la solución con la que cuenta la UPME para la protección del correo electrónico, de la red de comunicaciones, y la integración con el Firewall Palo Alto

OCTUBRE 2026

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera* ***"Copia No Controlada"****. La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.*

1. OBJETIVO DEL ESTUDIO

Adquirir el licenciamiento de la solución con la que cuenta la UPME para la protección del correo electrónico, de la red de comunicaciones, y la integración con el Firewall Palo Alto.

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.

En el marco del Plan Estratégico de Tecnologías de la Información – PETI, se describe la hoja de ruta a seguir para los años 2024 al 2026 las iniciativas y proyectos que buscan el cierre de brechas, mejorar la prestación de trámites y servicios a la ciudadanía y avanzar en la transformación digital de la Entidad. En tal sentido, la iniciativa PETI-5 busca "Impulsar el uso y apropiación de los productos, servicios y trámites que genera y ofrece la Entidad, a través de actividades de difusión, comunicación y mejoramiento de la página web de la Entidad".

La UPME requiere fortalecer los mecanismos de seguridad asociados al servicio de correo electrónico institucional, considerando que este constituye uno de los principales medios de comunicación y colaboración entre los funcionarios, contratistas, ciudadanos, entidades públicas y terceros interesados.
El correo electrónico es actualmente uno de los vectores más utilizados para la materialización de amenazas cibernéticas, tales como malware, ransomware, phishing, spear phishing, suplantación de identidad (spoofing), robo de credenciales y ataques de compromiso de correo corporativo (Business Email Compromise - BEC), los cuales pueden afectar la confidencialidad, integridad y disponibilidad de la información institucional, así como la continuidad de los servicios tecnológicos que soportan la operación de la entidad.

Aunque la entidad cuenta con mecanismos de seguridad para la protección de su infraestructura tecnológica, se hace necesario implementar capacidades especializadas de seguridad avanzada para el correo electrónico que permitan identificar, prevenir, analizar y mitigar amenazas cada vez más sofisticadas dirigidas a los usuarios institucionales y a los activos de información.

En este contexto, se requiere adquirir el licenciamiento de Sophos Central Email Advanced, solución especializada de seguridad para correo electrónico que proporciona funcionalidades de protección multicapa contra amenazas avanzadas, análisis de enlaces maliciosos en tiempo real, detección de archivos adjuntos maliciosos mediante técnicas avanzadas de inspección, protección contra ataques

Recuerde: Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.

de suplantación de identidad y herramientas centralizadas para la administración, monitoreo y gestión de eventos de seguridad asociados al correo electrónico institucional.

Es importante señalar que durante la vigencia 2025 la Entidad adquirió el licenciamiento para la protección de la red de comunicaciones con NDR (Detección y Respuesta de Red) de Sophos, la integración del Firewall con la solución de Sophos y la protección del tráfico de correo electrónico a través de la solución Email Advance de Sophos con un alcance de 520 buzones, lo anterior, a través del contrato CO1.PCCNTR.8550300 y el contrato CO1.PCCNTR.8543630. Se precisa que la solución de software adquirida con los contratos indicados cubren: 1) la protección de la entidad a través del sistema NDR, el cual detecta la actividad maliciosa en lo más profundo de la red que los endpoints y firewalls no pueden ver a través de análisis continuo del tráfico en busca de patrones sospechosos como actividad inusual; 2) la protección de los correos electrónicos para monitorear el tráfico entrante y saliente; y 3) la integración con el monitoreo central con el firewall Palo Alto. En una visualización sería:

Característica	Central Email Advanced - 200-499 users - Renovación	Central Network Detection and Response (NDR) - 200-499 users - Renovación
Objetivo	Protección del correo electrónico	Protección de la red de comunicaciones
Capa de seguridad	Email Security	Network Security
Qué protege	Correos entrantes y salientes	Tráfico de red y comunicaciones entre sistemas
Amenazas que detecta	Phishing, malware, spam, ransomware por correo, suplantación de identidad (BEC)	Movimiento lateral, comunicaciones maliciosas, ransomware, ataques internos y amenazas avanzadas
Fuente de análisis	Mensajes de correo electrónico	Tráfico de red y metadatos de comunicaciones
Tecnología	Sophos Central Email Advanced	Sophos NDR integrado con Sophos Central
Resultado	Evita que amenazas ingresen por correo	Detecta ataques que ya están ocurriendo dentro de la red

Estos sistemas se encuentran actualmente implementados y activos en la entidad, teniendo licenciamiento hasta el noviembre 11 del 2026, de los se requiere su renovación para continuar con la protección referida.

Por otro lado, y en una revisión efectuada de parte de la OTI, se denota la existencia de una necesidad para ampliar el licenciamiento previamente existente en lo que respecta a ampliar la protección de 260 cuentas de correo actualmente existentes a través del sistema Central Email Advanced de Sophos.

Recuerde: Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.

Así, y conforme a los señalado, para mayor comprensión del alcance de dicho licenciamiento, a continuación, se presenta descripción de cada uno:

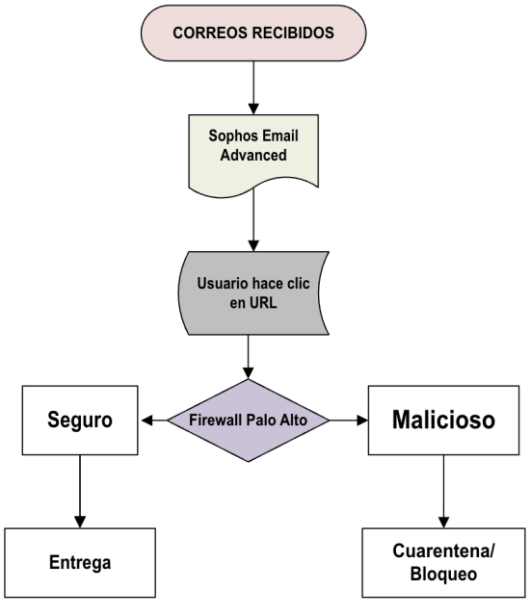
- **Seguridad del correo electrónico:** protección del phishing, detección de ataques de suplantación de identidad sin malware y de estafa por correo electrónico corporativo comprometido, bloquea ataques mediante análisis con Machine Learning del contenido del mensaje, autenticación de remitentes, protección de direcciones URL y espacios seguros en la nube. La solución de protección de correo escanea automáticamente los mensajes y archivos adjuntos en busca de datos sensibles con integración del cifrado. Cuenta con políticas de pérdida de datos DLP de múltiples reglas para grupos y usuarios individuales para garantizar la protección de información sensible en todos los correos y adjuntos.

- **NDR Network Detection and Response**: detecta la actividad maliciosa en lo más profundo de la red que los endpoints y firewalls no pueden ver, análisis continuo del tráfico en busca de patrones sospechosos, como actividad inusual que se origina en dispositivos desconocidos o no administrados, recursos no autorizados, nuevos servidores o movimientos de datos inesperados. Detectar rápidamente tráfico sospechoso o malicioso, con tecnologías de Deep Learning, inspección detallada de paquetes, análisis de cargas cifradas, análisis de nombres de dominio y potentes analíticas.

- **Integración de la solución de monitoreo central con el firewall Palo Alto**: la inclusión de la integración entre la solución de monitoreo central y el Firewall Palo Alto de la UPME dentro del alcance original de la oferta se sustenta técnicamente en la propia arquitectura nativa del servicio Sophos MDR. Esta solución está diseñada bajo un modelo agnóstico e interoperable de Detección y Respuesta Extendida (XDR), el cual contempla de manera predeterminada el ingesta, normalización y procesamiento de telemetría proveniente de cortafuegos de terceros mediante conectores e integraciones preconstruidas (API/Syslog) hacia la plataforma Sophos Central. Bajo este flujo operativo, la plataforma recibe de forma automatizada los eventos y alertas generados por el Firewall Palo Alto, aplicando algoritmos avanzados de filtrado, depuración y correlación cruzada de datos para eliminar falsos positivos y consolidar una visibilidad global del entorno. Posteriormente, aquellos incidentes que superan los umbrales de riesgo son escalados de forma transparente al centro de operaciones de seguridad (SOC) para su investigación y respuesta proactiva por parte de los analistas de Sophos, cumpliendo estrictamente con el objetivo de centralización, automatización de flujos de trabajo y refuerzo de las defensas sin requerir licencias de monitoreo adicionales.

El flujo que resume este proceso de seguridad se presenta a continuación:

Recuerde: Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.



Finalmente, la adquisición del licenciamiento para estas soluciones no solo es necesaria para cumplir con los estándares de seguridad y cumplimiento, sino que también es esencial para proteger los activos digitales de la UPME, garantizando la continuidad del negocio, preservando su reputación.

Aspecto regulatorio:

En Colombia, las entidades públicas obligadas a mantener y reportar información pública conforme a lo definido en el artículo 5 de la Ley 1712 de 2014, entre esas la UPME, se encuentran obligadas a mantener unas condiciones mínimas de seguridad digital como lo establece el artículo 6 y el anexo 3 de la Resolución MINTIC 1519 de 2020.

De esto, el anexo 3 de la Resolución MINTIC 1519 de 2020 es claro en definir en el numeral 3.2 las condiciones de seguridad digital que las entidades públicas deben cumplir, de los que deriva la necesidad jurídica de contar con sistemas, sean softwares y hardwares, que protejan las conexiones internas y externas de la entidad, estando entre las obligaciones a cargo de estas el adoptar las políticas para implementar un sistema de gestión de seguridad digital y de seguridad de la información (numeral 1).

Así las cosas, entonces, el uso de sistemas de protección para la conexión externa e interna a través de redes, correos electrónicos y demás, es fundamental para cumplir con los principios de seguridad, confidencialidad y transparencia establecidos en la legislación colombiana, asegurando el cifrado de los datos transmitidos en línea. Adicionalmente, el Decreto 620 de 2020, que refuerza la política de seguridad digital en el país, promueve la adopción de tecnologías que protejan la información y fortalezcan la confianza digital de los ciudadanos en los servicios públicos. Por tanto, la adquisición de este certificado responde a la obligación de garantizar la seguridad de las plataformas digitales en conformidad con los marcos regulatorios vigentes en Colombia.

Finalmente, el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC: Define directrices para la protección de la infraestructura tecnológica en entidades públicas.

Recuerde: Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.

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

1. Entregar 780 licencias del Central Email Advanced de Sophos para la protección de buzones de correo electrónico, las cuales, además de brindar la protección de correos, debe realizar filtros antispam, escaneado de malware, detección de URL maliciosas, reescritura de direcciones URL en el momento del clic, análisis de la reputación, detección de anomalías en encabezados, protección contra la suplantación de identidad, protección contra el phishing de suplantación de identidad con procesamiento del lenguaje natural, análisis del nombre mostrado (VIP y marcas), comprobaciones de dominios de imitación, prevención de fugas de datos, cifrado de mensajes y archivos adjuntos basado en imposición, sincronización de AD y otras funcionalidades.
2. Suministrar 315 licencias de una solución tipo NDR que permita supervisar la actividad de red en busca de patrones sospechosos y maliciosos detectando flujos de tráfico anormales de sistemas no gestionados, dispositivos IoT, recursos no autorizados, amenazas internas, ataques de día cero desconocidos y patrones inusuales en lo más profundo de la red.
3. Disponer de la plataforma que permite controlar el licenciamiento así como la generación de reportes producto del monitoreo que se realiza a los elementos que se cubren con el licenciamiento adquirido.
4. Monitorear 24x7 los elementos o servicios de la infraestructura tecnológica de la Entidad, objeto del presente proceso.
5. Contar con las actualizaciones permanentes que libere el fabricante de la solución adquirida.
6. Realizar transferencia de conocimiento hacia la Unidad en los términos de la oferta presentada por el proveedor.
7. Prestar el respectivo soporte técnico de la solución hasta la finalización del licenciamiento adquirido, 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 de la oferta presentada por el proveedor.
8. Cumplir con la Garantía y soporte técnico de fábrica por el tiempo contratado.
9. Cumplir con la oferta presentada.
10. Entregar a satisfacción de la Unidad Minero Energética -UPME- los productos y servicios establecidos en el alcance del presente proceso.
11. Garantizar que el licenciamiento que se adquiere en el presente proceso se integra y puede interoperar con los diferentes elementos y servicios tecnológicos de la infraestructura de TI de la Entidad.
12. Adoptar medidas inmediatas para mitigar el impacto, en caso de que se confirme una amenaza o incidente de seguridad.
13. Atender los acuerdos de niveles de servicio establecidos con el supervisor del contrato asignado por la UPME.
14. 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.
15. Realizar la gestión, monitoreo, correlación de eventos y resolución de eventos e incidentes de seguridad, sobre los elementos de la infraestructura tecnológica de la UPME, objeto del presente proceso.
16. 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.

Productos a entregar:

1. Certificado que contenga el número de licencias adquiridas y su respectiva vigencia.

Nº de licencias	Producto	Periodo
780	Central Email Advanced - 200-499 users – Renovación	Nov 2026 a Nov 2027
315	Central Network Detection and Response - 200-499 users - Renovación	Nov 2026 a Nov 2027

Entrega de bienes

El contratista deberá entregar el siguiente bien intangible: certificado de licenciamiento el cual se deberá ingresar al almacén.

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:

UNSPSC:
- 43233200 - Software de seguridad y protección
- 81111800 – Servicios de sistemas y administración de componentes de sistemas
- 81111801 – Seguridad de los computadores, redes o internet
- 81112208 – Mantenimiento de software de protección y seguridad

Deber de análisis de las Entidades estatales:

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), de acuerdo con la Ley 1341 de 2009, desarrolla políticas y planes enfocados a las Tecnologías de la Información y las Comunicaciones que constituyen un componente vital para el crecimiento y desarrollo del sector, con el fin de brindar acceso a toda la población, en el marco de la expansión y diversificación de las TIC, y conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de dicha ley, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

Con base en lo anterior, la UPME debe asegurar que su infraestructura cumpla con las garantías y los lineamientos de tecnología y seguridad necesarios acordes a los estándares de seguridad de la información como la norma técnica ISO/IEC 27001:2013, la ISO 22301:2012 y con ella establecer los controles adecuados para garantizar la confidencialidad, integridad y disponibilidad mitigando los riesgos identificados dentro la plataforma tecnológica de la UPME

Recuerde: Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.

Sustentación del porqué se requiere hacer una contratación directa:

De conformidad con lo establecido en el artículo 49 (Título IV, Capítulo 2) del Manual de Contratación adoptado por la Resolución UPME 578 de 2026, la modalidad de selección es DIRECTA, bajo la causal de: "49.4 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 licenciamiento de la solución con la que cuenta la UPME para la protección del correo electrónico, de la red de comunicaciones 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 VEINTIDÓS MILLONES CIENTO SESENTA Y SIETE MIL QUINIENTOS PESOS M/CTE. ($122.167.500) 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.

2. HISTÓRICO DE CONTRATACIÓN

Por parte de la UPME:

Incluir cuadro resumen de contrataciones anteriores que contenga la siguiente información:

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

Recuerde: Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.

Por parte de otras Entidades:

A continuación, se relacionan los Procesos de Contratación de otras Entidades Estatales que consultó la dependencia para identificar la manera en que se contrata el servicio, oportunidades de mejora y recopilar las buenas prácticas de contratación. En la página www.colombiacompra.gov.co – SECOP II, se encontró que durante los últimos años fueron adjudicados procesos de contratación similares

Incluir cuadro resumen de contrataciones por otras entidades que contenga la siguiente información:

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	RENOVACION 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

La Oficina de Tecnología de la Información adelantó el estudio de mercado solicitando cotizaciones, el día 14 de octubre del 2026, estás solicitudes fueron enviadas a través de correo electrónico en la cual se invitaron a 4 empresas:

- SODITEK
- Redes Tercer Milenio (RTM)
- GLOBALTEKSECURITY
- CYSTECNOLOGIA

Los oferentes que respondieron a esta solicitud, fueron:

- SODITEK

Recuerde: Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.

- RTM

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 de los oferentes que respondieron:

DESCRIPCIÓN	CANT	SODITEK	RTM
Central Network Detection and Response - 200-499 users - 12 MOS	315	$ 61.425.000	$ 51.187.500
Central Email Advanced - 200-499 users – 12 MOS - Renewal	780	$ 85.176.000	$ 70.980.000
Total		$ 146.601.000	$ 122.167.500

Una vez verificado el cumplimiento de los requisitos y especificaciones técnicas por parte de los oferentes, se determinó que las propuestas recibidas presentan condiciones equivalentes en cuanto al alcance, la calidad y las características de los servicios ofertados. De esto, y teniendo en cuenta las ofertas recibidas efectivamente, se efectuó el análisis de costos y establecer el menor precio como factor determinante para identificar la propuesta más favorable para la Entidad.

Como resultado del análisis comparativo, la oferta presentada por Redes Tercer Milenio (RTM) se identificó como la de menor valor económico entre las propuestas evaluadas, adicionalmente, se verificó que su oferta se ajusta al presupuesto asignado para la contratación y se revisó la experiencia del proveedor, con el propósito de establecer su idoneidad y capacidad para cumplir el objeto contractual.

Estos elementos permiten concluir que la propuesta seleccionada representa una alternativa conveniente para la UPME, al satisfacer los requerimientos definidos y favorecer el uso eficiente de los recursos públicos, sin comprometer las condiciones técnicas exigidas.

Para el caso concreto, y conforme a la validación realizada, se encuentra que la Sociedad Comercial REDES TERCER MILENIO S.A.S -RTM- fue constituida el 10 de julio de 1998 y matriculada el 21 de julio de 1998, teniendo presencia y trayectoria en el mercado por más de 20 años, cuyo objeto social está relacionado con el *diseño y montaje de soluciones de sistemas de hardware y software* así como la *comercialización de soluciones tecnológicas integrales en infraestructura informática,* como se acredita en el certificado de existencia y representación legal del 11 de octubre de 2026*.* A su vez cuenta con el certificado GOLD PARTNER de Sophos para el período abril 2026 a mayo de 2027.

En consecuencia, el criterio de selección aplicado fue el menor precio, considerando la equivalencia técnica de las propuestas y la conveniencia económica de la oferta presentada por REDES TERCER MILENIO S.A.S -RTM-, en concordancia con los principios de economía, eficiencia y eficacia que orientan la gestión contractual. Finalmente, se concluye que el valor estimado para la contratación es consistente con las condiciones identificadas en el mercado y con los precios de bienes o servicios de características similares, considerando las especificidades aplicables a la UPME.

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera* ***"Copia No Controlada"****. La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.*

4. ANEXOS

Se adjuntan los presupuestos enviados de manera oficial.

Recuerde: Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio oficial del Sistema de Gestión Institucional.