Datos del área Gestora.	**Dependencia solicitante:**	GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
	Nombre del servidor que diligencia la solicitud de información a proveedores:	LEIDY PAOLA GALINDO ACEVEDO

1. Descripción de la Necesidad que la Entidad Pretende Satisfacer y competencia funcional.

Que, el artículo 1° del Decreto 381 de 2012, el Ministerio de Minas y Energía "*tiene como objetivo formular, adoptar, dirigir y coordinar las políticas, planes y programas del Sector de Minas y Energía".*

Que, de conformidad con el artículo 17 del referido Decreto, modificado por el artículo 4 del Decreto 030 de 2022, son funciones de la Secretaría General, entre otras, las siguientes:

> *"(…) 5. Dirigir, coordinar y controlar los procesos de contratación del Ministerio en sus etapas precontractuales, contractuales y poscontractuales (sic), así como los contratos y convenios que deba suscribir o proponer el Ministerio.*
> *(…) 8. Proponer la adopción de políticas para el buen manejo y seguridad de la información sistematizada en el Ministerio, y promover el desarrollo e implementación de programas sistematizados*
> *(…)".*

Que, mediante Resolución No. 00631 de 2023 *"Por la cual se organizan los Grupos Internos de Trabajo al interior del Ministerio de Minas y Energía y se dictan otras disposiciones"*, se dispuso en su Artículo 11 la organización de los Grupos Internos de Trabajo del Despacho Secretaria General, incluido Grupo de Tecnologías de la Información y la Comunicaciones (GTICS), con las siguientes funciones:

> "*1. Liderar la estrategia digital del Ministerio y el Sector.*
> *2. Liderar la formulación e implementación de la arquitectura empresarial para la gestión digital en la entidad y de tecnologías de información en la entidad y proyectos conjuntos con el sector teniendo en cuenta los lineamientos gubernamentales y del CIO Sectorial.*
> *3. Asesorar al Ministerio en la definición de las políticas, planes, proyectos, programas y procedimientos inherentes al uso de tecnologías de información y comunicaciones.*
> *4. Diseñar, implementar e integrar soluciones digitales, basadas en procesos y procedimientos, para las dependencias del Ministerio.*
> *5. Establecer y ejecutar la estrategia de uso y apropiación de tecnologías digitales en la entidad.*
> *6. Asesorar en la definición de la estrategia de Seguridad y Privacidad de la Información acorde a las mejores prácticas.*
> *7. Implementar los lineamientos establecidos en la Política de Gobierno Digital*

propiciando la actualización tecnológica en la entidad y el Sector Minero Energético.
8. Proponer estrategias para la gestión de información en el Sector Minero Energético.
9. Liderar, coordinar y monitorear la infraestructura de tecnologías de la información y comunicaciones del Ministerio.
10. Formular e implementar el Plan Estratégico de Tecnologías de Información – PETI en la entidad.
11. Implementar planes y proyectos de infraestructura de Tecnologías de la Información - TI para la Entidad.
12. Definir, implementar y aplicar el modelo de contingencia, y alta disponibilidad de los servicios tecnológicos de la entidad.
13. Apoyar el desarrollo de las estrategias definidas por el CIO Sectorial.
14. Liderar el Comité interinstitucional de Tecnologías de Información y de Comunicación del Sector Minero Energético.
15. Las demás que le sean asignadas al grupo."

Que mediante el Decreto 767 de 2022 se establecieron los lineamientos generales de la Política de Gobierno Digital, la cual tiene la seguridad y privacidad de la información como uno de sus habilitadores y propende porque las entidades públicas presten servicios digitales confiables y seguros. En concordancia con ello, el Ministerio debe asegurar que su infraestructura tecnológica mantenga condiciones óptimas de operación, actualización, soporte y protección, de manera que se garanticen la continuidad de los servicios digitales y la adecuada gestión de los riesgos asociados a la seguridad de la información.

Que, asimismo, en cumplimiento de la Política Nacional de Confianza y Seguridad Digital adoptada en el Documento CONPES 3995 de 2020, del Decreto 338 de 2022 y de la Resolución 500 de 2021 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, que adopta el Modelo de Seguridad y Privacidad de la Información (MSPI), el Ministerio se encuentra obligado a implementar controles técnicos y administrativos que garanticen la protección, resiliencia y defensa de su infraestructura tecnológica frente a amenazas cibernéticas.

Que la presente adquisición se enmarca en el objetivo específico *"Aumentar el nivel de implementación de los modelos definidos en el Marco de Referencia de Arquitectura Empresarial."*, correspondiente al proyecto de inversión *"FORTALECIMIENTO DE LA CAPACIDAD DEL MINISTERIO DE MINAS Y ENERGÍA PARA IMPLEMENTAR DE MANERA EFECTIVA LA POLÍTICA DE GOBIERNO DIGITAL NACIONAL"*, con código BPIN 202400000000198-02, a cargo del Grupo de Tecnologías de la Información y las Comunicaciones. Conforme a la MGA, dicho proyecto contempla el siguiente objetivo, producto y entregable, con sus respectivas fechas:

OBJETIVO ESPECIFICO DEL PROYECTO DE INVERSIÓN:	Aumentar el nivel de implementación de los modelos definidos en el Marco de Referencia de Arquitectura Empresarial.
Producto	Servicios tecnológicos
Entregable	Adquirir bienes y servicios para la operación y soporte de los proyectos de base tecnológica en la Entidad.
Iniciativas	GO001 Adquisición de software y renovación

	de suscripciones
Fecha de Inicio	1 de enero 2025
Fecha de finalización	31 de diciembre 2028
Meta 2026	92,5%

Así mismo, el proceso a adelantar para la adquisición y renovación de las soluciones de ciberseguridad para la gestión de exposición, detección y respuesta ante amenazas sobre los activos del Ministerio se alinea con el objetivo de aumentar el nivel de implementación de los modelos definidos en el Marco de Referencia de Arquitectura Empresarial del proyecto BPIN 202400000000198-02, y se materializa como servicios tecnológicos que permiten adquirir los bienes y servicios para la operación y soporte de los proyectos de base tecnológica de la Entidad, en desarrollo de la iniciativa GO001 *"Adquisición de software y renovación de suscripciones".* En ese sentido, la contratación contribuye directamente al cumplimiento de la meta prevista para la vigencia 2026, en la medida en que asegura la continuidad y ampliación de las capacidades tecnológicas que soportan la operación de la Entidad mediante la renovación de suscripciones y la adquisición de software especializado. Al mismo tiempo, fortalece el objetivo del proyecto, por cuanto incorpora controles de visibilidad, protección y respuesta frente a amenazas sobre la infraestructura y los sistemas que procesan la información institucional y del sector minero-energético, con lo cual consolida la seguridad y privacidad de la información como habilitador de la Política de Gobierno Digital, cuya implementación efectiva constituye la finalidad del proyecto de inversión.

Que, en desarrollo de lo anterior y en cumplimiento de las funciones del Grupo de Tecnologías de la Información y las Comunicaciones, el Ministerio requiere fortalecer de manera integral la gestión de los riesgos de seguridad digital sobre sus activos tecnológicos y usuarios, a partir del diagnóstico de sus capacidades actuales de seguridad. Dicho diagnóstico evidencia la necesidad de contar con dos capacidades complementarias: la primera en un ámbito preventivo, consistente en identificar, evaluar y priorizar de forma continua las vulnerabilidades y exposiciones de los activos antes de que sean aprovechadas; y la segunda, de detección y respuesta, orientada a identificar, investigar y contener oportunamente las amenazas que se materialicen sobre estaciones de trabajo, los servidores y demás fuentes de la infraestructura. Las cantidades requeridas para cada componente se dimensionaron conforme al inventario de activos tecnológicos de la Entidad. En consecuencia, la presente solicitud de información comprende los siguientes componentes:

Componente 1. Renovación y ampliación de la plataforma de gestión de exposición y vulnerabilidades.

En el año 2023 el Ministerio adquirió la plataforma Tenable con el fin de contar con una solución especializada para la identificación, clasificación y seguimiento de las vulnerabilidades técnicas presentes en su infraestructura tecnológica y en sus sistemas de información. Desde su implementación, la plataforma ha sido operada por el Grupo de Tecnologías de la Información y las Comunicaciones, dependencia responsable de la seguridad de la información en la Entidad, y los análisis ejecutados con ella han permitido evidenciar el estado real de exposición de los activos tecnológicos del Ministerio. Durante la vigencia del contrato anterior se identificaron y gestionaron cerca de dos mil doscientas sesenta y tres (2.263) vulnerabilidades, de las cuales cincuenta y cuatro (54) eran de severidad crítica, con riesgo inminente de explotación según el

catálogo de vulnerabilidades explotadas conocidas (KEV) de CISA y la métrica VPR. La identificación temprana de estas brechas permitió aplicar los parches y ajustes de configuración requeridos antes de que pudieran ser aprovechadas para accesos no autorizados, secuestro de información o indisponibilidad de servicios esenciales.

A partir de los resultados de cada análisis, el Grupo TIC prioriza los hallazgos según su nivel de criticidad (crítica, alta, media y baja), aplica las actualizaciones, parches y ajustes de configuración correspondientes, y realiza nuevos escaneos para verificar el cierre efectivo de cada vulnerabilidad. Ahora bien, el número de vulnerabilidades identificadas tiende a crecer sin que ello signifique un deterioro de la gestión, pues cada año se publican nuevas vulnerabilidades a nivel mundial (solo en 2024 se registraron más de cuarenta mil (40.000) en la base de datos CVE) y la infraestructura de la Entidad evoluciona con la incorporación de nuevos servidores, aplicaciones, servicios y equipos. En ese sentido, una mayor cantidad de hallazgos refleja una mayor capacidad de detección y visibilidad sobre los activos, lo que permite actuar antes de que estas debilidades sean explotadas.

No obstante, el alcance actual de la plataforma Tenable con la que cuenta el Ministerio instalada en su infraestructura, se limita a operar únicamente como un escáner de red interna, presentando una brecha crítica de visibilidad, pues no analiza aplicaciones web ni detecta la superficie de ataque expuesta en Internet, y carece de correlación de rutas de ataque (*Attack Paths*), generando alertas aisladas sin contexto de riesgo necesario para priorizar adecuadamente su atención por parte de la Entidad.

Por ello, se requiere renovar el licenciamiento de la plataforma y actualizarla a Tenable One Advance, garantizando la continuidad operativa sobre la base instalada, con el aprovechamiento de los agentes, políticas, configuraciones y datos históricos existentes, y consolidando bajo una única consola los siguientes tres módulos integrados:

- **Gestión de vulnerabilidades en activos TI (Tenable VM):** ochocientos (800) activos.
- **Gestión de vulnerabilidades en aplicaciones web (Tenable WAS):** cincuenta (50) FQDN.
- **Gestión de superficie de ataque externa (Tenable ASM):** ciento cincuenta (150) activos públicos.

Esta plataforma unifica la métrica global de riesgo (*Tenable Exposure Score* - TES) e incorpora capacidades de inteligencia artificial para la priorización y correlación automatizada de hallazgos críticos.

Componente 2. Adquisición de una solución de detección y respuesta extendida (XDR).

La Entidad cuenta con una infraestructura tecnológica integrada por equipos de usuario final, servidores y otros componentes que soportan el funcionamiento de sus sistemas y servicios tecnológicos. Para garantizar su adecuado funcionamiento y proteger la información institucional no basta con identificar vulnerabilidades: es necesario, además, prevenir la ejecución de programas o software malicioso y detectar a tiempo las amenazas que lleguen a materializarse sobre estos equipos, de modo que puedan investigarse y contenerse antes de que afecten la operación o comprometan la información. El Ministerio no cuenta actualmente con una solución que le permita correlacionar los eventos de seguridad provenientes de sus distintas fuentes, investigar los incidentes y ejecutar acciones de respuesta desde una consola centralizada, por

lo que esta capacidad constituye una necesidad nueva dentro de su esquema de seguridad digital.

Por lo anterior, el Ministerio requiere una solución tecnológica de protección avanzada, monitoreo, detección, investigación y respuesta ante amenazas para estaciones de trabajo y servidores, complementaria a sus capacidades actuales de seguridad, dimensionada en setecientos cincuenta (750) equipos de usuario final o computadores y doscientos ochenta (280) para servidores definidas por el Ministerio. La solución deberá facilitar:

- la identificación de comportamientos anómalos;
- el análisis contextual de eventos provenientes de múltiples fuentes;
- la investigación de incidentes;
- la ejecución de acciones de contención, sin requerir la sustitución de las plataformas de seguridad existentes.

Con esta solución se busca mejorar la prevención y detección de amenazas, reducir los riesgos de seguridad y contar con mecanismos de respuesta oportuna ante posibles incidentes, de acuerdo con las necesidades y características de la infraestructura tecnológica de la Entidad.

Que la falta de estas capacidades implicaría, en el caso del Componente 1, la pérdida inmediata de visibilidad sobre el estado de exposición de los activos tecnológicos del Ministerio y, de no renovarse la plataforma, de los datos históricos de vulnerabilidades acumulados; y en el caso del Componente 2, limitaría la posibilidad de detectar, investigar y responder oportunamente ante incidentes de seguridad. En ambos casos aumentaría el riesgo de afectación de los activos digitales y de la continuidad de los servicios institucionales, y se comprometería el cumplimiento de los controles técnicos exigidos por el MSPI y por el CONPES 3995 de 2020.

Que, conforme a lo expuesto, ambos componentes atienden una misma necesidad: fortalecer y ampliar las capacidades institucionales de detección, identificación, análisis, mitigación y respuesta frente a vulnerabilidades técnicas y amenazas cibernéticas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de los servicios tecnológicos misionales de la Entidad. Se trata, además, de componentes complementarios, pues mientras la plataforma de gestión de exposición y vulnerabilidades identifica las debilidades que requieren tratamiento antes de ser explotadas, la solución XDR identifica las actividades sospechosas y las amenazas que se materializan sobre los elementos de la infraestructura, de manera que su integración permite contextualizar cada detección con la información de vulnerabilidades del activo afectado y priorizar la respuesta según el riesgo real de seguridad digital del Ministerio.

Que, en consecuencia, las soluciones requeridas deberán integrarse, mediante conectores, interfaces y API documentadas, con las herramientas de seguridad, monitoreo, orquestación e inteligencia de amenazas con que ya cuenta la Entidad, sin exigir su reemplazo ni duplicar innecesariamente su adquisición. En particular, la solución del Componente 2 deberá poder integrarse con la plataforma de gestión de exposición del Componente 1.

Que la estructuración de ambos componentes como una sola necesidad atiende los principios de planeación, economía y eficacia que rigen la función administrativa y la contratación estatal, consagrados en el artículo 209 de la Constitución Política y en el artículo 25 de la Ley 80 de 1993. Esta estructuración permite gestionar de manera integral un mismo riesgo, adelantar un único análisis del sector y del mercado, y asegurar desde la planeación la compatibilidad e

integración entre las soluciones. A su vez, con el fin de no restringir la participación de los proveedores, cada componente se describe y cotiza de manera independiente, de modo que los interesados puedan presentar información para uno o ambos componentes, según su especialidad.

Que se verificó en la Tienda Virtual del Estado Colombiano, administrada por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, que a la fecha no existe un Acuerdo Marco de Precios ni otro instrumento de agregación de demanda vigente que cubra la totalidad del objeto de la presente contratación, con su alcance y sus especificaciones técnicas. Si bien se encuentra vigente el Instrumento de Agregación de Demanda de Software por Catálogo II, con plazo para colocar órdenes de compra hasta el 21 de noviembre de 2027 y cobertura de software y servicios complementarios, este no satisface la necesidad de la Entidad en ninguno de sus dos componentes, dado que la obligación de acudir a los instrumentos de agregación de demanda se predica únicamente cuando el bien o servicio requerido se encuentra cubierto por ellos, lo que en el presente caso no ocurre, por las razones que se exponen a continuación.

En el Componente 1, el fabricante Tenable y sus referencias no se encuentran incluidos en el catálogo vigente, y las herramientas allí dispuestas no son técnicamente homologables a la solución requerida. A diferencia de las soluciones del catálogo, limitadas a escaneos puntuales y aislados o a módulos desarticulados de múltiples fabricantes, la necesidad de la Entidad corresponde a la renovación y ampliación de la plataforma Tenable instalada en el Ministerio, actualizándola a Tenable One Advance. Esta plataforma opera bajo un modelo de gestión continua de la exposición a amenazas, que correlaciona de forma nativa, bajo una única consola y un repositorio de datos común, la gestión de vulnerabilidades en activos TI, en aplicaciones web y en la superficie de ataque externa. Asimismo, calcula dinámicamente el nivel de riesgo institucional mediante una métrica unificada de exposición, prioriza las vulnerabilidades con base en información diaria de explotación activa e integra capacidades de análisis de rutas de ataque y de inteligencia artificial, que permiten anticipar el encadenamiento de vectores de compromiso sobre los activos críticos de la Entidad antes de su explotación. Sustituir esta solución por herramientas genéricas del catálogo fragmentaría la visibilidad en silos de gestión independientes, haría perder la base instalada y los históricos analíticos consolidados de la Entidad, y comprometería la capacidad del Ministerio para cuantificar y gestionar el riesgo cibernético de manera centralizada.

En el Componente 2, la necesidad no se agota en el suministro de licencias de software, pues corresponde a una solución especializada de detección y respuesta extendida en modalidad SaaS. Esta solución debe operar conjuntamente con la solución antivirus existente sin sustituirla, ingerir y correlacionar telemetría de múltiples fuentes de la infraestructura del Ministerio, integrarse con las tecnologías de seguridad con que cuenta la Entidad y con la plataforma del Componente 1, conservar los datos durante toda la vigencia de la suscripción e incorporar capacidades de automatización de la respuesta, inteligencia de amenazas e inteligencia artificial, conforme al anexo técnico. Por tratarse de una solución de ciberseguridad que interactúa directamente con los mecanismos de protección implementados, su funcionamiento debe ser compatible con la infraestructura tecnológica existente, de manera que se conserven las configuraciones de seguridad y se garantice la continuidad de los servicios. En consecuencia, la solución requerida no puede adquirirse a través del instrumento en las condiciones de integración, implementación y soporte que exige la necesidad de la Entidad, pues la adquisición de referencias de licenciamiento por catálogo no garantiza su despliegue, integración y operación conforme a los requerimientos del anexo técnico.

Adicionalmente, para ambos componentes el alcance comprende la entrega y activación del licenciamiento, la implementación, configuración, integración, pruebas y puesta en operación de las soluciones, la documentación y la transferencia de conocimiento, así como el soporte técnico, las actualizaciones y la garantía durante la vigencia del licenciamiento. Estos servicios deben prestarse bajo condiciones particulares definidas en el anexo técnico, como la implementación por fases con un equipo de trabajo especializado, la integración con la infraestructura del Ministerio y un soporte sujeto a acuerdos de niveles de servicio con un régimen propio de compensaciones, que no corresponden a los servicios complementarios estandarizados del instrumento. Por lo anterior, y sin que ello implique eludir los instrumentos de agregación de demanda, la Entidad adelantará el proceso de contratación a través de la plataforma SECOP II. (https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/acuerdos-marco)

Que la activación para el licenciamiento, las actualizaciones y el soporte de ambos componentes permitirá mantener la continuidad de las capacidades de protección y de gestión de exposición, conforme a las apropiaciones y autorizaciones presupuestales correspondientes. Ese horizonte protege la inversión que la Entidad realiza en la implementación y puesta en funcionamiento de las soluciones, así como el acervo de datos acumulado en ellas.

2. Descripción del objeto a contratar, con sus especificaciones, autorizaciones, permisos y licencias requeridos para su ejecución.	
2.1. Descripción del Objeto a contratar:	Adquirir y renovar una solución tecnológica para el análisis e identificación temprana de riesgos y vulnerabilidades en activos digitales y usuarios, facilitando su evaluación, priorización y mitigación oportuna.
Alcance del objeto:	El alcance comprende dos componentes complementarios. El primero es la renovación y ampliación del licenciamiento de la plataforma de gestión de exposición y vulnerabilidades instalada y en operación en el Ministerio, y su actualización a Tenable One Advance, para la gestión de vulnerabilidades en activos TI, aplicaciones web y superficie de ataque externa, sin pérdida de datos históricos ni de configuraciones existentes. El segundo es la adquisición de una solución de detección y respuesta extendida (XDR) para estaciones de trabajo y servidores, integrada con las herramientas de seguridad con que cuenta la Entidad. Para ambos componentes, el alcance incluye la entrega y activación del licenciamiento, la implementación, configuración, integración, pruebas y puesta en operación de las soluciones, la documentación y la transferencia de conocimiento, así como el soporte técnico, las actualizaciones y la garantía durante la vigencia del licenciamiento. Las especificaciones técnicas detalladas, las cantidades, los requisitos mínimos de cada componente y condiciones de aceptación se encuentran precisados en la FICHA DE CARACTERÍSTICAS TÉCNICAS - ANEXO TÉCNICO - XDR Y TENABLE.

<table>
<tr><td>Clasificador de Bienes y Servicios:</td><td>
<table>
<tr><th>Código UNSPSC</th><th>Segmento</th><th>Familia</th><th>Clase</th></tr>
<tr><td>81111500</td><td>81 – Servicios basados en ingeniería, investigación y tecnología</td><td>11 – Servicios informáticos</td><td>15 - Ingeniería de software o hardware</td></tr>
<tr><td>81112200</td><td>81 – Servicios basados en ingeniería, investigación y tecnología</td><td>11 – Servicios informáticos</td><td>22 – Mantenimiento y soporte de software</td></tr>
<tr><td>81112500</td><td>81 – Servicios basados en ingeniería, investigación y tecnología</td><td>11 – Servicios informáticos</td><td>25 – Servicios de alquiler o arrendamiento de licencias de software de computador</td></tr>
<tr><td>43231500</td><td>43 – Difusión de tecnologías de información y telecomunicaciones</td><td>23 – Software</td><td>15 – Software funcional específico de la empresa</td></tr>
<tr><td>43233200</td><td>43 – Difusión de tecnologías de información y telecomunicaciones</td><td>23 – Software</td><td>32 – Software de seguridad y protección</td></tr>
</table>
</td></tr>
<tr><td>2.3.1 Plazo de ejecución del contrato:</td><td>El plazo de ejecución del contrato será de un (1) mes o hasta el 31 de diciembre de 2026, lo que primero ocurra, contado a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento y ejecución. Dentro de dicho plazo el contratista deberá entregar y activar el licenciamiento correspondiente a cada componente y ejecutar las actividades de implementación, configuración, integración, pruebas y puesta en operación de la solución, conforme a lo previsto en el anexo técnico.

NOTA 1: La vigencia del licenciamiento para cada uno de los componentes será determinable por una periodicidad entre doce (12), veinticuatro (24) o treinta y seis (36) meses, siendo este último plazo el límite máximo de duración, el cual se establecerá posteriormente, según el resultado del proceso de cotización y sondeo del mercado.

NOTA 2: Para efectos del sondeo de mercado, el proveedor deberá cotizar de manera obligatoria los tres (3) escenarios de vigencia —doce (12), veinticuatro (24) o treinta y seis (36) meses—, discriminando el valor de cada componente en cada escenario. La cotización que omita alguno de los escenarios no podrá ser considerada para el análisis comparativo.</td></tr>
<tr><td>2.3.2 Lugar de ejecución del contrato:</td><td>El contrato se ejecutará en la ciudad de Bogotá D.C.</td></tr>
</table>

	Las actividades de entrega y activación del licenciamiento, implementación, configuración, integración, pruebas, puesta en operación, administración y soporte técnico podrán adelantarse de forma remota, a través de los accesos que autorice la Entidad y bajo los controles de seguridad de la información definidos por el Ministerio de Minas y Energía. Las actividades que requieran presencia del contratista, como la transferencia de conocimiento, las intervenciones sobre la infraestructura local o la atención de casos que así lo exijan, se coordinarán previamente con el supervisor del contrato y se desarrollarán en las instalaciones del Ministerio ubicadas en el Centro Administrativo Nacional – CAN, Calle 43 No. 57-31 de Bogotá D.C., o en aquellas donde llegaren a ubicarse sus dependencias. Los costos de desplazamiento correrán por cuenta del contratista.
2.3.3 Documentos técnicos requeridos. (Permisos, autorizaciones, licencias cuando se requieran):	Ver: FICHA DE CARACTERÍSTICAS TÉCNICAS - ANEXO TÉCNICO - XDR Y TENABLE

3. Condiciones y Características Técnicas requeridas para el proceso de contratación

Ver: FICHA DE CARACTERÍSTICAS TÉCNICAS - ANEXO TÉCNICO - XDR Y TENABLE

4. Equipo de trabajo y perfil que se requiere para el proceso de contratación (si aplica)

Ver: FICHA DE CARACTERÍSTICAS TÉCNICAS - ANEXO TÉCNICO - XDR Y TENABLE

5. Información adicional para la generación de la solicitud de información a proveedores en SECOP II

5.1 Bienes y servicios (TODA la Lista de artículos a cotizar)

No. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad de medida
1	81111500 81112200 81112500 43231500 43233200	**COMPONENTE 1.** Renovación de la suscripción SaaS de la plataforma Tenable de la Entidad y su actualización a Tenable One Advance. Licenciamiento para mil (1.000) activos: ochocientos (800) activos TI, cincuenta (50) FQDN y ciento	1.000	Unidad

		cincuenta (150) activos públicos.		
2	81111500 81112200 81112500 43231500 43233200	**COMPONENTE 2.** Adquisición de una solución de detección y respuesta extendida (XDR). Licenciamiento para mil treinta (1.030) equipos: setecientos cincuenta (750) equipos de usuario final o computadores y doscientos ochenta (280) servidores.	1.030	Unidad

6. Obligaciones Generales

Además de las obligaciones inherentes a la naturaleza y esencia del presente contrato, EL CONTRATISTA se obliga a:

1. Cumplir el objeto del contrato con plena autonomía técnica, administrativa y financiera, bajo su responsabilidad en las condiciones de calidad y oportunidad, de conformidad con la oferta presentada, los documentos precontractuales, las especificaciones técnicas, con sus respectivas adendas y modificaciones y los demás documentos que hagan parte integral del mismo.
2. Contratar, conforme a lo dispuesto en la propuesta presentada, bajo su absoluta responsabilidad, el personal suficiente e idóneo que sea necesario para la cabal ejecución del objeto de este contrato.
3. Adelantar los trámites y cumplir los requisitos necesarios para la oportuna legalización y ejecución del contrato dentro de los plazos establecidos, suscribiendo oportunamente el acta de inicio del contrato, las actas derivadas de mesas de trabajo, las actas que resulten con ocasión y ejecución del contrato, las modificaciones a que haya lugar y el acta de liquidación de este.
4. Atender y responder por su cuenta y riesgo, por los accidentes personales y eventualidades que le ocurran al personal que desarrolla el objeto del contrato.
5. Acreditar ante la supervisión con cada solicitud de pago, el cumplimiento de sus obligaciones con el Sistema de Seguridad Social Integral y aportes parafiscales, respecto de sí mismo y del personal que destine a la ejecución del contrato, mediante certificación suscrita por el revisor fiscal, cuando este exista de acuerdo con los requerimientos de ley, o por el representante legal, de conformidad con el artículo 50 de la Ley 789 de 2002 y el artículo 23 de la Ley 1150 de 2007.
6. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones, malentendidos y entorpecimientos durante la ejecución del contrato.
7. Reportar de manera inmediata al supervisor del contrato del Ministerio de Minas y Energía, cualquier novedad o anomalía que pueda afectar la ejecución del contrato.
8. Cumplir con las normas de seguridad industrial aplicables, durante la ejecución del contrato.
9. Cumplir con los estándares mínimos de seguridad y salud en el trabajo según la RESOLUCIÓN 0312 DE 2019, “por la cual se define los Estándares Mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo” y/o de aquellas normas que la sustituyan, modifiquen o adicionen.

10. Guardar total reserva de la información que por razón de sus obligaciones y desarrollo de sus actividades obtenga. Esta es de propiedad del Ministerio de Minas y Energía y sólo por expreso requerimiento de autoridad competente podrá ser divulgada, así como no utilizar documentos y/o información suministrada por el Ministerio para fines distintos a los del objeto contractual.
11. Responder civil y penalmente por sus acciones y omisiones en la actuación contractual en los términos de la ley.
12. Constituir las garantías requeridas por el Ministerio y mantenerlas actualizadas durante la ejecución y vigencia del contrato, así como realizar las modificaciones que se presenten en la ejecución del mismo, dentro de los 3 días hábiles siguientes a la suscripción del contrato y/o de su modificación, o cuando sea requerido por el supervisor del contrato.
13. Cumplir con la responsabilidad administrativa y laboral del personal que destine a la ejecución del contrato, conforme a la Ley 100 de 1993, la Ley 789 de 2002, la Ley 797 de 2003 y demás normas concordantes, así como aquellas que las sustituyan, modifiquen o adicionen. El contratista entiende y acepta que no existirá vínculo laboral alguno entre el MME y el personal que el contratista designe para el cumplimiento del objeto contractual.
14. Garantizar el cabal cumplimiento de las normas que se deriven de la naturaleza del objeto contractual, así como las de seguridad industrial y demás normas indicadas en casos de contingencia.
15. Dar cumplimiento a lo establecido en la Directiva Presidencial 09 de 2020 “LINEAMIENTOS PARA EL PAGO A LOS PROVEEDORES DEL ESTADO” y/o de aquella que la sustituya, modifique o adicione.
16. Acatar y aplicar de manera diligente las observaciones, lineamientos y recomendaciones impartidas por el supervisor del contrato del Ministerio de Minas y Energía.
17. Las demás inherentes al objeto y a la naturaleza del contrato y aquellas indicadas por el Supervisor para el cabal cumplimiento del objeto del contrato.

7.Obligaciones específicas

Para garantizar el cumplimiento integral del contrato, el contratista tendrá a su cargo las siguientes obligaciones específicas:

Obligaciones comunes a los dos componentes:

1. Entregar y activar, a nombre del Ministerio de Minas y Energía, el licenciamiento de cada componente en las cantidades y por la vigencia establecidas en los documentos contractuales. El licenciamiento deberá ser original, legítimo, vigente y habilitado para uso institucional, y el contratista deberá entregar las constancias emitidas por el fabricante o su canal autorizado, en las que consten las cantidades, la cobertura y las fechas de vigencia.
2. Presentar el plan de trabajo y el cronograma de ejecución dentro de los tres (3) días calendario siguientes a la suscripción del acta de inicio, para aprobación del supervisor del contrato, y realizar los ajustes que este solicite.
3. Ejecutar las actividades de implementación, configuración, integración, pruebas y puesta en operación de las soluciones. Las intervenciones que puedan afectar servicios productivos deberán realizarse en las ventanas autorizadas por la Entidad y conforme a las buenas prácticas del fabricante.
4. Ejecutar las pruebas de aceptación definidas en el anexo técnico y presentar sus resultados, como requisito para el recibo a satisfacción de cada componente.
5. Entregar la documentación de la implementación, que comprende, como mínimo: a) el plan de trabajo; b) la arquitectura de la solución; c) las evidencias de pruebas; d) las actas; e) los manuales

y la documentación de configuración; f) informe final del resultado de implementación. Esta documentación no deberá contener contraseñas, llaves privadas ni otros secretos.

6. Realizar la transferencia de conocimiento al personal designado por la Entidad, en los términos del anexo técnico.
7. Prestar el soporte técnico durante toda la vigencia del licenciamiento, de acuerdo con los acuerdos de niveles de servicio establecidos en el anexo técnico. El soporte comprende el diagnóstico y la corrección de fallas, la documentación de los casos y de las acciones adelantadas, la actualización de configuraciones, la gestión del escalamiento con el fabricante cuando sea necesario, así como las demás actividades comprendidas en el anexo técnico.
8. Suministrar y aplicar, durante la vigencia del licenciamiento, las actualizaciones de producto y de seguridad liberadas por el fabricante.
9. Presentar informes con la periodicidad que acuerde con el supervisor del contrato, sobre: a) el estado y la cobertura de las soluciones; b) los hallazgos y alertas relevantes; c) los casos atendidos; las recomendaciones; d) actualizaciones sobre configuraciones realizadas.
10. Notificar de inmediato a la Entidad cualquier incidente, falla crítica o vulnerabilidad de las soluciones que pueda afectar la seguridad de la información del Ministerio.
11. Suscribir el acuerdo de confidencialidad que disponga la Entidad y dar cumplimiento a la Ley 1581 de 2012 y a las políticas de seguridad y privacidad de la información del Ministerio respecto de la información a la que tenga acceso.
12. Presentar, al término del plazo de ejecución, la evidencia documentada que acredite la activación y el correcto funcionamiento de la totalidad de las capacidades contratadas, es decir, capturas de consola, reporte de licencias activas y acta de aceptación suscrita por la Entidad. Esa evidencia deberá alojarse en el repositorio que indique el Ministerio.
13. Entregar, al vencimiento de la vigencia del licenciamiento, la configuración, los reportes y los registros de las soluciones, y acompañar la transición hacia una nueva solución o proveedor sin interrumpir la protección de los activos.

Obligaciones del Componente 1 – Renovación y ampliación de la plataforma de gestión de exposición y vulnerabilidades:

14. Garantizar la continuidad operativa de la plataforma durante la renovación, sin pérdida de datos históricos de vulnerabilidades, grupos de activos, etiquetas, políticas de escaneo, credenciales almacenadas ni configuraciones de integraciones activas, y validar con el fabricante la ruta de actualización aplicable a la instalación existente en la Entidad.
15. Ampliar el licenciamiento de gestión de vulnerabilidades en activos TI hasta la cantidad prevista en el anexo técnico, y validar la conectividad y la evaluación autenticada sobre la totalidad de los activos en alcance.
16. Poner en operación la gestión de vulnerabilidades en aplicaciones web para los cincuenta (50) FQDN y la gestión de la superficie de ataque externa para los ciento cincuenta (150) activos públicos que defina la Entidad, y validar la cobertura total de los dominios y activos autorizados.
17. Activar y mantener operativas, durante la vigencia del licenciamiento, las capacidades de protección de la identidad digital institucional previstas en el anexo técnico.
18. Las demás inherentes al objeto y a la naturaleza del contrato y aquellas indicadas por el Supervisor para el cabal cumplimiento del objeto del contrato.

Obligaciones del Componente 2 – Adquisición de una solución de detección y respuesta extendida (XDR)

18. Desplegar los agentes o sensores de la solución en las estaciones de trabajo y servidores definidos por la Entidad, de manera que operen conjuntamente con la solución antivirus existente, sin requerir su sustitución.
19. Definir, configurar y poner en operación, en conjunto con la Entidad y durante la implementación, los playbooks de automatización para la respuesta ante eventos de seguridad, a necesidad de la Entidad, y documentarlos.
20. Integrar la solución, cuando sea técnicamente viable y esté autorizado por la Entidad, con las herramientas existentes de monitoreo, automatización e inteligencia de amenazas, incluida la plataforma de gestión de exposición del Componente 1.
21. Acompañar integralmente a la entidad durante las etapas de afinamiento y paso a producción de la solución contratada. Asimismo, prestar acompañamientos ante eventos críticos o incidentes de seguridad que se presenten.
22. Las demás inherentes al objeto y a la naturaleza del contrato y aquellas indicadas por el Supervisor para el cabal cumplimiento del objeto del contrato.

¿Permitir visitas al lugar de ejecución?, en caso de que se permitan, agregue la información que considere para realizar las visitas	No aplica.
Fecha y hora límite para responder la solicitud de información	Hasta las 17:00 horas después de 5 días hábiles contados a partir del día siguiente de la publicación en SECOP II de la solicitud de información de proveedores.

Firma Responsable: _____

Nombre: **LEIDY PAOLA GALINDO ACEVEDO**

Cargo: **Coordinadora Grupo de Tecnologías de la Información y las Comunicaciones – TICS**

Proyectó: Hernán Humberto Garzón Bonilla – Contratista / Grupo de Tecnologías de la Información y las Comunicaciones
Proyectó: Diego Ferney Martínez Cuadros – Contratista / Grupo de Tecnologías de la Información y las Comunicaciones
Proyectó: Camilo Andrés Pinzón Rincón – Contratista / Grupo de Tecnologías de la Información y las Comunicaciones
Revisó: Juan José Cedeño López– Técnico Administrativo / Grupo de Tecnologías de la Información y las Comunicaciones
Revisó: Paola Andrea Ramírez Pereira – Contratista / Grupo de Tecnologías de la Información y las Comunicaciones

REVISÓ
PAOLA ANDREA RAMIREZ PEREIRA
CONTRATISTA
06-11-2026 15:44:35