



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

RESPUESTA A OBSERVACIONES PRESENTADAS PARA EL PROCESO QUE TIENE POR OBJETO:
“CONTRATAR LOS SERVICIOS DE CENTRO DE OPERACIONES DE SEGURIDAD, ADMINISTRACIÓN, PROTECCIÓN, PRUEBAS Y GESTIÓN DE INCIDENTES DE SEGURIDAD RELACIONADAS CON LA PLATAFORMA TECNOLÓGICA QUE SOPORTAN LAS ACTIVIDADES MISIONALES Y DE FISCALIZACIÓN DE LA AGENCIA NACIONAL DE MINERÍA ANM.” LÍNEAS PAA: 613000125 Y 130010925

OBSERVACIONES PRESENTADAS POR CROSSBORDER TECH

OBSERVACIÓN No. 1:

“Numeral 6.4.2 Certificaciones relacionadas con el Operaciones de Seguridad) del proponente SOC (Centro de Operaciones de Seguridad) del proponente.

Texto del requisito: Acreditación como MSSP - Managed Security Service Provider, por el fabricante del SIEM (Gestión de Eventos e Información de Seguridad Security Information and Event Management) que sea utilizado para prestar el servicio.”

Observación: Solicitamos amablemente a la entidad aclarar el alcance del numeral, en el sentido de precisar si la acreditación MSSP exigida debe corresponder al fabricante del SIEM que el proponente utilice durante la fase inicial de transición (bajo modalidad SaaS, de propiedad de la ANM), o si debe corresponder necesariamente al fabricante Fortinet, en tanto la solución SIEM definitiva a operar durante la mayor parte del plazo contractual será FortiSIEM, adquirida por la propia Entidad en el marco de este proceso.

RESPUESTA DE LA ENTIDAD: SE ACLARA

La Agencia Nacional de Minería aclara que la exigencia de la acreditación o alianza como **MSSP (Managed Security Service Provider)** expedida por el fabricante del SIEM está directamente relacionada con la idoneidad técnica, el nivel de soporte, la escalabilidad y las capacidades operativas requeridas para administrar, desplegar e integrar la solución tecnológica propia y definitiva del contrato, la cual corresponde a **FortiSIEM**.

En consecuencia, la acreditación MSSP presentada **debe corresponder al fabricante Fortinet**, garantizando que el oferente cuenta con las competencias, el respaldo directo de fábrica, los escalamientos de nivel 3 y la experiencia certificada para la puesta en marcha, *tuning* y operación continua del entorno **FortiSIEM** en la máquina virtual de la Entidad.

OBSERVACIONES PRESENTADAS POR SECURESOFT COLOMBIA S.A.S

OBSERVACIÓN No. 1:

1. Principio de Neutralidad Tecnológica y Pluralidad

Referencia: Anexo Técnico, Cuadro de Cantidades (Ítems 8 y 9).

Observación: Se observa que en el cuadro de cantidades y en el alcance del objeto se predetermina la adquisición de marcas y productos específicos como "FortiSIEM" y "FortiPAM".



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Al tratarse de un proceso de Subasta Inversa para bienes de características técnicas uniformes, la normativa colombiana exige que las especificaciones sean objetivas y funcionales. Nombrar fabricantes específicos restringe la libre concurrencia de otros proponentes que representan tecnologías líderes y que podrían ofrecer mejores condiciones de desempeño.

Se solicita amablemente a la Entidad definir estos requerimientos de forma funcional (ej. "Adquisición de solución SIEM con capacidad de 1000 EPS"), permitiendo el ofrecimiento de soluciones equivalentes o superiores que cumplan con los patrones de desempeño requeridos.

RESPUESTA DE LA ENTIDAD:

NO SE ACOGE LA SOLICITUD. La Entidad mantiene la exigencia técnica de las soluciones específicas FortiSIEM y FortiPAM.

Es preciso aclarar al observante que el principio de pluralidad de oferentes no se limita a la coexistencia de distintas marcas o fabricantes en el mercado, sino a la posibilidad real de que múltiples proveedores compitan en igualdad de condiciones dentro del proceso de selección. En este caso, tanto **FortiSIEM** como **FortiPAM** son productos de comercialización abierta a través de un ecosistema amplio y diverso de canales, distribuidores y mayoristas autorizados en Colombia. Por lo tanto, no existe restricción a la libre concurrencia ni direccionamiento hacia un proponente en particular, garantizando la participación transparente de múltiples firmas bajo el mecanismo de Subasta Inversa.

La Agencia Nacional de Minería cuenta actualmente con una arquitectura perimetral y de ciberdefensa consolidada bajo la plataforma Fortinet (incluyendo Firewalls FortiGate, WAF FortiWeb, analizadores FortiAnalyzer y clientes ZTNA). La adquisición de las tecnologías FortiSIEM y FortiPAM no obedece a un capricho de marca, sino a la necesidad técnica y operativa de lograr la unificación de la infraestructura tecnológica como elemento estratégico de la estrategia de ciberseguridad.

La integración nativa entre estas herramientas ofrece las siguientes ventajas operativas y presupuestales críticas para la ANM:

1. **Visibilidad y Correlación Directa:** La integración nativa de FortiSIEM y FortiPAM con el ecosistema existente elimina capas intermedias de traducción de logs, simplifica el envío de telemetría y reduce la latencia en la detección y contención de amenazas.
2. **Eficiencia en la Respuesta a Incidentes:** Permite la ejecución de acciones automatizadas de respuesta (Playbooks / SOAR nativo) directamente sobre los dispositivos de red y seguridad existentes sin incurrir en costos adicionales de desarrollo, conectores de terceros o licenciamiento por integración de APIs.
3. **Optimización de Costos y Complejidad Operativa:** Mantener una arquitectura unificada evita sobrecostos por licenciamiento de conectores propietarios, reduce la curva de aprendizaje de los administradores y minimiza el riesgo de brechas de configuración derivadas de la gestión de múltiples plataformas heterogéneas.

Por consiguiente, la decisión de la Entidad responde estrictamente a la necesidad de preservar la interoperabilidad, la eficiencia operativa y la economía de la infraestructura de ciberseguridad, cumpliendo con la justificación técnica que soporta la contratación.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

OBSERVACIÓN No. 2:

Referencia: Numeral 7.8 y Descripción de Infraestructura.

Observación: La Agencia solicita un SIEM con capacidad para 50 dispositivos. No obstante, el diagnóstico de infraestructura de la ANM reporta un inventario de 30 servidores físicos, 250 servidores virtuales (VMware), 48 servidores Oracle VM y 65 Switches, sumando más de 390 activos críticos.

Se solicita amablemente a la entidad confirmar cómo garantiza la visibilidad total de su infraestructura si la herramienta solicitada solo cubriría menos del 20% de los activos reportados? Se advierte una inconsistencia de dimensionamiento que generaría brechas de seguridad críticas. Se sugiere ampliar la capacidad funcional para cubrir el 100% de la infraestructura misional descrita en los estudios previos.

RESPUESTA DE LA ENTIDAD:

NO SE ACOGE LA SOLICITUD. La Entidad aclara la diferencia conceptual entre el inventario de activos de TI y el alcance de fuentes del SIEM, manteniendo las especificaciones técnicas publicadas.

La Entidad aclara al observante que existe una clara distinción técnica entre el **inventario total de activos de TI** de la organización y el **conjunto de fuentes estratégicas que deben enviar eventos e ingresar directamente al SIEM**. La inclusión del inventario detallado dentro de los documentos del proceso tiene como fin exclusivo brindar al oferente un contexto macro y un panorama amplio sobre la dimensión de la infraestructura tecnológica de la Agencia, permitiéndole entender la arquitectura general donde operará el servicio.

Criterio de Monitoreo Basado en Riesgo y Fuentes Estratégicas:

Las mejores prácticas en ciberseguridad y gestión de eventos (SIEM) establecen que el monitoreo centralizado no requiere la ingesta indiscriminada de eventos de la totalidad de endpoints o componentes pasivos, sino la selección analítica de **fuentes de información de alto impacto y capas de agregación estratégica**.

La capacidad solicitada de 50 dispositivos (y su correspondiente licenciamiento de EPS) está correctamente dimensionada para la ingesta de las fuentes clave identificadas por el equipo técnico de seguridad de la ANM, tales como:

1. Cortafuegos perimetrales (NGFW) y controladores de red principales.
2. Controladores de dominio e infraestructura crítica de identidad (Active Directory / PAM).
3. Servidores de base de datos misionales, WAF y portales web expuestos a Internet.
4. Agregadores de eventos y consolas de gestión centralizada que consolidan alertas de capas inferiores (ej. hipervisores o defensas Endpoint) sin necesidad de conectar individualmente cada nodo o VM.

Por consiguiente, el alcance dimensionado garantiza la visibilidad de los vectores de ataque y componentes críticos de la infraestructura sin generar sobrecostos por licenciamiento superfluo, manteniendo el equilibrio técnico y financiero del contrato.

OBSERVACIÓN No. 3:

Informacion publica



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Referencia: Numeral 7.1 y 7.2 del Anexo Técnico.

Observación: La arquitectura propuesta concentra la seguridad perimetral, la correlación de eventos y la gestión de accesos en un único fabricante. En ciberdefensa, esto genera un punto único de falla estructural. Si el motor de detección de dicho fabricante presenta una vulnerabilidad, toda la cadena de blindaje de la Agencia quedaría comprometida simultáneamente.

Se recomienda a la ANM adoptar un modelo de "Doble Defensa", permitiendo que los componentes de monitoreo (SIEM) y gestión de privilegios (PAM) sean de fabricantes distintos a la capa perimetral. Esto garantiza que las capacidades de detección sean complementarias y no dependan de un único set de firmas o algoritmos, blindando de manera más robusta los datos críticos.

RESPUESTA DE LA ENTIDAD:

NO SE ACOGE LA SOLICITUD. La Entidad agradece la observación técnica formulada por el interesado, pero se ratifica en la necesidad de mantener la integración homogénea de los componentes sobre la misma arquitectura tecnológica del fabricante (Fortinet). La selección del modelo de arquitectura responde a una evaluación profunda de las necesidades operativas, la capacidad de respuesta y la madurez tecnológica específica de la ANM.

Aunque el concepto de heterogeneidad ("Doble Defensa") es respetable en ciertos entornos, en la práctica operativa de la ANM la adopción de una arquitectura unificada (Ecosistema / Security Fabric) ofrece beneficios técnicos superiores que mitigan los riesgos operativos:

1. **Respuesta Automatizada (SOAR) y Visibilidad Unificada:** La integración nativa entre el Firewall, WAF, ZTNA, FortiSIEM y FortiPAM permite la ejecución automática de acciones de contención (aislamiento de IP, bloqueo de usuarios comprometidos, revocación de credenciales privilegiadas) en tiempo real y sin necesidad de desarrollar ni mantener scripts o conectores personalizados de terceros.
2. **Eliminación de Puntos Ciegos e Interoperabilidad Inmediata:** La correlación de eventos entre fuentes de una misma arquitectura reduce de manera significativa los falsos positivos y acelera el tiempo medio de detección y respuesta (MTTD / MTTR), al compartir telemetría y contexto de amenazas de forma estandarizada.
3. **Continuidad Operativa y Gestión Centralizada:** Contar con un ecosistema integrado simplifica la administración, la gestión de parches, las actualizaciones de firmas y la atención de soporte técnico ante incidentes complejos, evitando la dispersión de responsabilidades entre múltiples fabricantes.

La ANM aclara que la arquitectura de seguridad institucional no es monolítica ni depende de un único estándar, ya que convive y se complementa con otras capas tecnológicas independientes ya desplegadas en la Entidad (como las soluciones de seguridad para nube/endpoint de Microsoft Defender y herramientas de gestión de vulnerabilidades tipo Vicarius), garantizando la diversidad de vectores de detección sin sacrificar la eficiencia operativa en la infraestructura de red y control de acceso. Por lo tanto, la Entidad ratifica las condiciones técnicas publicadas en los pliegos del proceso



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

OBSERVACIÓN No. 4:

Referencia: Requisito de posicionamiento Gartner para SIEM [Contexto de Selección Objetiva].

Observación: Existe una contradicción en el estándar de calidad exigido. Mientras que para el SIEM se requieren categorías de "Líder" o "Retador", para la gestión de accesos privilegiados (PAM) se preddefine una herramienta (FortiPAM) que no figura en los cuadrantes de liderazgo de analistas independientes como Gartner.

Sugerencia: Para continuar con el proceso de madurez tecnológica, se solicita permitir la competencia de tecnologías "Top Tier" (Líderes en Gartner) que ofrezcan capacidades superiores de analítica de comportamiento, asegurando que la tecnología sea proporcional a la criticidad de los activos de la Agencia, incluyendo la escalabilidad a sistemas OT.

RESPUESTA DE LA ENTIDAD:

NO SE ACOGE LA SOLICITUD. La Entidad aclara la confusión en la que incurre el observante al mezclar la naturaleza técnica de ambas soluciones, y se ratifica en las condiciones exigidas y aclarará al observante que existe una confusión conceptual en su observación al equiparar los requisitos de dos soluciones con propósitos operacionales completamente distintos:

1. **SIEM (Security Information and Event Management):** Corresponde a una plataforma de correlación, análisis masivo de eventos y monitoreo centralizado de ciberseguridad.
2. **PAM (Privileged Access Management):** Corresponde a una solución de gestión, control, auditoría y aseguramiento de credenciales de cuentas con privilegios elevados. No es una herramienta de monitoreo de eventos general de red ni compete en la categoría de SIEM.

Respecto a la afirmación sobre el posicionamiento de mercado, se le precisa al oferente que FortiSIEM sí forma parte del Cuadrante Mágico de Gartner para SIEM (*Magic Quadrant for Security Information and Event Management*), habiendo sido reconocido de manera consecutiva en la categoría de "Challenger" (Retador). Por lo tanto, la tecnología solicitada para la infraestructura propia de la ANM cumple estrictamente con los estándares de reconocimiento de mercado de analistas independientes exigidos dentro del proceso contractual. La adquisición e implementación de FortiPAM responde a la estrategia de unificación del control de accesos privilegiados integrado nativamente al ecosistema de red y ZTNA de la Entidad. Exigirle a PAM el mismo criterio de acreditación en un reporte específico de SIEM es técnicamente improcedente por tratarse de categorías de mercado completamente diferentes.

Por lo anterior, se mantienen inalteradas las especificaciones y exigencias consignadas en los pliegos de condiciones.

OBSERVACIÓN No. 5:

Referencia: Ítem 8 - Adquisición de SIEM en VM.

Observación: El proceso planea migrar de un SIEM SaaS a un modelo de propiedad virtualizada (VM) dentro del clúster de la Agencia. Esto traslada al contratista y a la ENTIDAD la carga administrativa de gestionar el hardware, el hipervisor y el desempeño de la VM, distrayendo el foco de la detección de incidentes.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Se sugiere amablemente a la ENTIDAD considerar un modelo MSSP (Managed Security Service Provider) basado en SaaS no solo en el inicio sino durante toda la vigencia del contrato. Bajo este esquema, el contratista asume la responsabilidad total de la disponibilidad de la plataforma, eliminando riesgos de indisponibilidad por fallas en la infraestructura local de la ANM y optimizando el uso de los recursos de inversión. El contratista deberá garantizar la entrega de logs en caso que la ENTIDAD lo requiera.

RESPUESTA DE LA ENTIDAD:

NO SE ACOGE LA SOLICITUD. La Entidad se ratifica en el esquema planteado: uso transitorio del modelo SaaS para la fase de migración/empalme y posterior despliegue e integración en la infraestructura de máquina virtual (VM) **propietaria de la ANM** (FortiSIEM).

La decisión estratégica de adquirir e implementar un SIEM propio en la infraestructura virtualizada de la ANM garantiza la **soberanía tecnológica y la custodia total de los registros (logs) y telemetría de seguridad**. Un esquema SaaS/MSSP permanente condiciona la retención, el acceso histórico y la auditoría de los datos a la continuidad del contrato con un tercero. Contar con una plataforma propia (FortiSIEM VM) asegura que, al finalizar cualquier relación contractual, la inteligencia acumulada, las reglas de correlación, las políticas construidas y la trazabilidad histórica permanezcan bajo el control exclusivo de la Entidad.

Las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) del Gobierno Nacional exigen a las entidades públicas la adopción de controles de preservación, inalterabilidad y custodia de la evidencia digital. Mantener la plataforma en el clúster privado de la Entidad fortalece el cumplimiento de los esquemas de gobernanza, auditoría interna y requerimientos de entes de control sin depender de repositorios o nubes de terceros.

Se le aclara al observante que el hecho de que la plataforma FortiSIEM opere en la infraestructura virtualizada de la ANM no exime al contratista seleccionado de las obligaciones de administración, soporte técnico, tuning, creación de reglas de correlación y gestión de parches/actualizaciones de la solución durante la vigencia del contrato. Por lo tanto, la carga operativa especializada sigue estando cubierta por el servicio administrado contratado, sin restar foco a la detección y respuesta ante incidentes. Por lo anterior, la Entidad mantiene inalteradas las condiciones establecidas en los documentos del proceso.

OBSERVACIÓN No. 6:

Referencia: Plazo de ejecución y servicio SaaS de transición.

Observación: Se contempla un periodo de 2 meses para el servicio SaaS actual mientras se realiza la implementación de la nueva tecnología.

Considerando la complejidad de migrar reglas de correlación, logs históricos e integración de fuentes en Nube Privada, un plazo de 30 días para la puesta en marcha definitiva es técnicamente insuficiente para garantizar una transición sin puntos ciegos, luego la transición a una herramienta en OnPremise va a requerir un doble esfuerzo que se traduce en costos adicionales para la entidad,

Sugerencia: Se solicita extender el periodo de coexistencia y soporte del SaaS de transición a un mínimo de 4 meses, y permitir ofertar la continuidad en herramientas SaaS para facilitar su transición, asegurando la continuidad total del monitoreo 7x24 durante la fase crítica de estabilización de la nueva plataforma.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

RESPUESTA DE LA ENTIDAD:

NO SE ACOGE LA SOLICITUD. La Entidad se ratifica en el plazo de dos (2) meses establecido para el servicio transitorio SaaS y en el cronograma de empalme e implementación de la solución definitiva.

La definición del periodo de dos (2) meses para el servicio SaaS transitorio responde a una planificación técnica previa alineada con la complejidad real de la infraestructura de la ANM. Dentro de la metodología de proyectos de ciberseguridad, un plazo de 60 días es plenamente suficiente para ejecutar las fases de despliegue de la máquina virtual (VM), aprovisionamiento, ajuste de políticas (*tuning*), migración de reglas clave de correlación e ingesta progresiva de logs desde las fuentes estratégicas definidas.

El ítem correspondiente al servicio SaaS transitorio (Ítem 5) se encuentra estrictamente dimensionado acorde con las necesidades y requerimientos de la Entidad. Extender dicho servicio a cuatro (4) meses implicaría alterar la estructura financiera del proceso, desviando recursos presupuestales destinados a las soluciones definitivas y generando un sobre costo no contemplado en la estructuración del estudio previo.

El perfil exigido para el proponente y su equipo de trabajo presupone la capacidad idónea, experiencia y metodologías ágiles para llevar a cabo proyectos de migración de SIEM dentro de los tiempos estipulados por la Entidad, evitando dilaciones innecesarias en la adopción de la infraestructura propia.

Por lo tanto, la Entidad ratifica el plazo de dos (2) meses para el servicio SaaS de transición y las condiciones de entrega publicadas en los Pliegos de Condiciones

OBSERVACIONES PRESENTADAS POR WEXLER S.A.S

OBSERVACIÓN No. 1:

1. Capacidad de licenciamiento y procesamiento de EPS

“1 x FortiSIEM en VM para 50 dispositivos y 1000 EPS con soporte a 12 meses y servicio de implementación y puesta en marcha.”

Asimismo, el numeral 7.2.26 establece:

El proveedor deberá garantizar que la solución SIEM este en capacidad de coleccionar, procesar, monitorear y correlacionar más de 3000 EPS sin filtrar y filtrados 512 EPS diarios.”

Observación:

Se solicita a la Entidad aclarar la capacidad de licenciamiento y procesamiento requerida para la solución FortiSIEM, teniendo en cuenta que se establece la adquisición de una licencia para 1.000 EPS, pero simultáneamente se exige capacidad para procesar más de 3.000 EPS sin filtrar y 512 EPS filtrados. Esta definición es necesaria para realizar el dimensionamiento técnico y económico adecuado de la solución.

RESPUESTA DE LA ENTIDAD:



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

SE ACLARA que La adquisición de licenciamiento inicial para el servidor FortiSIEM en máquina virtual corresponderá al tope base de 1.000 EPS contratados (licencia adquirida). Respecto a la cifra expresada en el numeral 7.2.26 (capacidad de procesamiento de 3.000 EPS sin filtrar y 512 EPS filtrados), esta corresponde a la **capacidad técnica de rendimiento/hardware (throughput)** que debe soportar la arquitectura de la instancia VM provisionada para procesar picos de ráfagas sin caída de servicios. La facturación/licencia licenciada exigida en el Ítem 8 es de 1.000 EPS para 50 dispositivos.

OBSERVACIÓN No. 2:

2. Alta disponibilidad y recuperación de desastres

Texto del pliego: “1 x FortiSIEM en VM para 50 dispositivos y 1000 EPS con soporte a 12 meses.”

Asimismo, el numeral 7.2.15 establece:

“La solución de recolección y correlación de eventos (SIEM) debe soportar esquemas de Alta Disponibilidad (Activo-Activo) y Recuperación de Desastre.”

Observación:

Se solicita aclarar si la Entidad requiere la implementación efectiva de una arquitectura de alta disponibilidad activo-activo y recuperación de desastres, o únicamente que el producto ofertado soporte técnicamente dichas funcionalidades.

RESPUESTA DE LA ENTIDAD:

SE ACLARA que La Entidad solicita una (1) sola instancia/licencia de FortiSIEM en VM. La condición establecida en el numeral 7.2.15 se refiere a la capacidad nativa del producto/software ofertado de soportar arquitecturas de Alta Disponibilidad (HA) y Disaster Recovery (DR) en caso de que la Entidad decida escalarlo a futuro. Para efectos de este contrato, la implementación en la infraestructura de la ANM será de una instancia única (Stand-alone / VM) sin despliegue de clúster redundante secundario.

OBSERVACIÓN No. 3:

3. Infraestructura para FortiSIEM y colectores

Texto del pliego: “La entidad tiene como propósito adquirir e implementar una solución SIEM propia dentro de su infraestructura tecnológica, compuesta por una (1) instancia SIEM virtualizada.”

Asimismo: “El oferente debe realizar la configuración de los colectores y cualquier configuración para la prestación de monitoreo, administración, correlación y gestión de eventos de seguridad.”

Observación:

Se solicita confirmar si la ANM suministrará la infraestructura virtual necesaria para la implementación de FortiSIEM y de los colectores requeridos, incluyendo recursos de procesamiento, memoria RAM, almacenamiento, interfaces de red, hipervisor, sistema operativo y conectividad. En caso de que la ANM no suministre la infraestructura virtual requerida, se solicita aclarar si el proponente podrá ofertar la solución FortiSIEM incluyendo el hardware necesario. De ser así, agradeceríamos confirmar si la Entidad cuenta con



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

disponibilidad de espacio en rack, alimentación eléctrica, conectividad y demás condiciones necesarias para su instalación física en el centro de datos de la ANM.

RESPUESTA DE LA ENTIDAD:

SE ACLARA que la Agencia Nacional de Minería (ANM) suministrará la infraestructura virtual requerida (hipervisor VMware, procesamiento CPU, memoria RAM, almacenamiento en SAN y direccionamiento/conectividad en su Data Center). El contratista únicamente debe entregar el licenciamiento del producto FortiSIEM en VM, los ejecutables/plantillas OVA para su despliegue y ejecutar el servicio de instalación, configuración, tuning y puesta en marcha. No se requiere la oferta de componentes de hardware físico ni espacio en rack por parte del proponente.

El proponente también debe realizar la configuración de colectores o supervisores necesarios para la implementación de la solución bajo las mismas condiciones establecidas anteriormente.

OBSERVACIÓN No. 4:

1. Modalidad de despliegue de la solución

Texto del pliego: “Adquisición, implementación, puesta en marcha, transmisión de conocimiento o capacitación y soporte por 12 meses para la solución de acceso privilegiado FORTIPAM.”

Observación:

Se solicita a la Entidad aclarar la modalidad de despliegue requerida para la solución FortiPAM, indicando si debe ser suministrada mediante appliance físico, máquina virtual instalada en la infraestructura de la ANM o desplegada sobre infraestructura de nube pública. Esta definición es necesaria para establecer la arquitectura, el licenciamiento y los componentes que deberán incluirse en la oferta.

RESPUESTA DE LA ENTIDAD:

SE ACLARA que la Agencia Nacional de Minería (ANM) suministrará la infraestructura virtual requerida (hipervisor VMware, procesamiento CPU, memoria RAM, almacenamiento en SAN y direccionamiento/conectividad en su Data Center). El contratista únicamente debe entregar el licenciamiento del producto FortiPAM en VM, los ejecutables/plantillas OVA para su despliegue y ejecutar el servicio de instalación, configuración, tuning y puesta en marcha. No se requiere la oferta de componentes de hardware físico ni espacio en rack por parte del proponente.

OBSERVACION 5.

En caso de requerirse FortiPAM en modalidad virtual, solicita confirmar si la ANM suministrará la infraestructura virtual (hipervisor, vCPU, RAM, almacenamiento, red y conectividad).

RESPUESTA DE LA ENTIDAD:

SE ACOGE LA SOLICITUD Y SE ACLARA.

RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

La Agencia Nacional de Minería suministrará la totalidad de la infraestructura virtual (hipervisor VMware, procesamiento, memoria RAM, almacenamiento en SAN/disco y direccionamiento IP) necesaria para el despliegue de la solución FortiPAM.

OBSERVACION 6.

Solicita precisar el período de retención para las grabaciones de sesiones y logs de FortiPAM, así como el volumen de sesiones y si el almacenamiento será provisto por la ANM.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

El periodo de retención para las grabaciones de sesiones, auditorías y registros generados por FortiPAM será de tres (3) meses en línea como mínimo para consulta directa en la plataforma. La infraestructura de almacenamiento (espacio en disco SAN) necesaria para alojar dichas grabaciones y evidencia digital será suministrada por la ANM dentro de su centro de cómputo.

OBSERVACION 7. MONITOREO DE MICROSOFT DEFENDER, INTUNE, SENTINEL Y ANTIVIRUS ALTERNO

Solicita aclarar si el alcance sobre Microsoft Defender, Intune, Sentinel y Antivirus alterno incluye exclusivamente monitoreo y escalamiento, o si abarca administración directa, afinamiento y gestión de políticas. Asimismo, consulta por la marca del antivirus alterno y el acceso a licencias.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

Alcance: El alcance del contratista comprende la configuración de conectores, monitoreo 7 *24, análisis de eventos, correlación de alertas, afinamiento de reglas (*tuning*) y atención/escalamiento de incidentes generados por Defender for Office 365, Defender for Endpoint, Intune, Microsoft Sentinel y la plataforma de antivirus alterno. La gestión de políticas administrativas de fondo se coordinará con los administradores de la ANM.

Es importante aclarar que si bien es cierto el alcance no comprende la configuración, administración directa de estas plataformas, como proveedor de seguridad si debe participar en las sesiones relacionadas con estas como apoyo, asesoría y soporte ante cualquier cambio o configuración que sea requerida.

Estas plataformas deben quedar configuradas como parte del correlacionamiento de eventos al FORTISIEM que debe ser implementado dentro de los dos primeros meses al inicio del contrato.

Antivirus Alterno y Licenciamiento: La ANM aportará el 100% de los accesos, perfiles de administración e integraciones necesarias. Para el antivirus alterno de servidores, la Entidad ya dispone del licenciamiento activo (no requiere cotizar software). (Remitirse a la Respuesta No. 29 de *Grupo Licitaciones G* y No. 4 de *TIVIT Colombia*).

OBSERVACION 8. RENOVACIÓN DE LICENCIAMIENTO FORTINET



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Solicita suministrar los números de serie (Serial Numbers) de los equipos Fortinet a renovar (2 NGFW 1100E, 2 FortiWeb 1000E, 1 FortiAnalyzer 300G, ZTNA 1700 Endpoints).

RESPUESTA DE LA ENTIDAD: SE ACLARA

- La Agencia Nacional de Minería publicó en el ANEXO Técnico los números seriales de los dispositivos objeto de renovación de licenciamiento. Sugerimos remitirse a dicho documento.

OBSERVACION 9.

Observación del Oferente: Solicita aclarar si la renovación debe realizarse bajo un esquema de coterminación para que todas las suscripciones finalicen en una misma fecha.

RESPUESTA DE LA ENTIDAD : SE ACLARA.

- La renovación de los productos y suscripciones Fortinet debe realizarse por una vigencia de doce (12) meses contados a partir de la fecha de finalización de cada producto, el cual se publica en el ANEXO TECNICO. La cotización oficial ante el fabricante/distribuidor se estructurará bajo el esquema de coterminación, tomando como fecha objetivo de vencimiento doce meses contados a partir de la fecha de activación coordinada en el acta de inicio contractual.

OBSERVACION 10.- PRUEBAS DE PENETRACIÓN O ETHICAL HACKING

Se Solicita aclarar si las pruebas de penetración sobre 10 direcciones IP internas/externas corresponden al mismo alcance de los 10 portales públicos o si es un alcance adicional.

RESPUESTA DE LA ENTIDAD : SE ACOGE LA SOLICITUD Y SE ACLARA.

- Se aclara al oferente que las evaluaciones sobre los diez (10) portales públicos de la ANM constituyen el núcleo de las pruebas de penetración / Ethical Hacking a nivel aplicativo (Caja Negra / Caja Gris). Las diez (10) direcciones IP (internas o externas) corresponden a los puntos de enlace, servidores o componentes de infraestructura que soportan dichos portales web, por lo que no constituyen un alcance desproporcionado o independiente, sino la infraestructura técnica directamente asociada a la ejecución del análisis sobre las 10 aplicaciones web contratadas.
- Se Aclara que las pruebas de EH son un componente diferente a las pruebas de vulnerabilidades correspondiente a 100 lp internas.

OBSERVACION 11- PRUEBA DE INGENIERÍA SOCIAL

Solicita aclarar la aplicabilidad del requisito *Certificate of CVE Compatibility - MITRE*, señalando que se orienta a gestión de vulnerabilidades y no a plataformas de phishing/ingeniería social.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

- La Entidad aclara que el certificado de compatibilidad CVE de MITRE aplica específicamente para las herramientas y plataformas utilizadas en el Análisis de Vulnerabilidades técnicas (100 IPs), y no es una condición exigible de manera estricta para el motor de envío de campañas de phishing / simulación de ingeniería social. Dicho requisito se acota a los componentes de escaneo y correlación de vulnerabilidades de la oferta.

OBSERVACION 12- ASSESSMENTS DE SEGURIDAD PERIMETRAL

Solicita aclarar cuáles dispositivos se incluyen en los dos (2) Assessments perimetrales (FortiGate, FortiWeb, ZTNA) e inventario de configuraciones.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

- El alcance de los dos (2) Assessments de Seguridad Perimetral (uno al inicio y el segundo a los 6 meses) comprende la totalidad de la capa perimetral activa de la ANM, la cual está conformada por los dos (2) Firewalls FortiGate 1100E, los dos (2) FortiWeb 1000E y la plataforma ZTNA/FortiAnalyzer. Dicha revisión incluye la auditoría de políticas, detección de reglas solapadas o en desuso y verificación de efectividad de accesos.

OBSERVACION 13- DIAGNÓSTICO INICIAL DE SEGURIDAD

Solicita precisar si el diagnóstico inicial del primer mes es una evaluación general/documental o si incluye pruebas técnicas, evitando duplicidad con los assessments y análisis de vulnerabilidades.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

- El Diagnóstico Inicial de Seguridad (a entregar en el mes 1) corresponde a una evaluación estratégica, documental y de postura general de ciberseguridad alineada con las guías del MSPI/MIPG de la ANM. Este entregable no duplica las pruebas técnicas, sino que consolida los hallazgos provenientes del primer Assessment Perimetral, el escaneo de vulnerabilidades inicial y la revisión de procesos/arquitectura, generando un documento ejecutivo con el plan de acción priorizado para la gestión del contrato durante los 12 meses.

OBSERVACIONES PRESENTADAS POR GRUPO LICITACIONES G

OBSERVACIÓN No. 1:

Documento: Proyecto de Pliego de Condiciones.

Tema: Documento de anexo para inscripción de terceros. Página: 54.

Texto del documento: "(...) El interesado deberá diligenciar el Anexo Inscripción de Terceros según corresponda.)"



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Observación y Solicitud: El Pliego de Condiciones menciona dentro de los requisitos/documentos a diligenciar por parte del interesado el denominado un Anexo de Inscripción de Terceros. No obstante, revisada minuciosamente la totalidad de los documentos del proceso publicados en la plataforma SECOP II, se evidencia que dicho anexo no fue adjuntado ni se encuentra disponible para su descarga. Adicionalmente, el pliego no precisa con claridad cuáles sujetos (proponente plural, integrantes, subcontratistas) deben acreditar esta condición ni la forma adecuada de hacerlo.

Con el fin de dar cumplimiento al principio de Transparencia que reza el art. 24 de la Ley 80 de 1993 que señala que los pliegos de condiciones deben definir reglas objetivas, claras, completas y precisas para que los interesados puedan elaborar sus ofertas en igualdad de condiciones y sin ambigüedades. Y al derecho a la Información Pública y al debido proceso que consagran los arts. 29 y 209 de la constitución nacional, la entidad tiene la obligación de poner a disposición de los proponentes toda la documentación indispensable para la conformación de la propuesta ya que el exigir un documento no publicado o no reglamentado debidamente vulnera la objetividad del proceso.

Por lo anterior, solicitamos respetuosamente a la entidad:

1. Publicar y/o adjuntar en la plataforma del proceso el archivo correspondiente al Anexo de Inscripción de Terceros para su oportuno diligenciamiento.

2. En su defecto, o de manera complementaria, aclarar e indicar expresamente en el Pliego Definitivo y/o Respuesta a Observaciones:

¿Quiénes están obligados a presentar o acreditar dicho requisito?

¿Cuál es el procedimiento exacto y la documentación equivalente aceptada en caso de que el interesado ya se encuentre registrado previamente ante la Entidad?

RESPUESTA DE LA ENTIDAD:

SE ACOGE LA SOLICITUD Y SE ACLARA.

Con la publicación de los pliegos de condiciones definitivos, la Entidad pondrá a disposición de todos los interesados a través de la plataforma SECOP II el formato oficial del "Anexo de Inscripción de Terceros" para su correspondiente diligenciamiento.

Se aclara que dicho anexo debe ser diligenciado y firmado por el representante legal del proponente. Dicho documento es un requisito de registro y gestión administrativa interna de la ANM para la creación del tercero en los sistemas financieros e institucionales, por lo cual no se considera la existencia de documento equivalente.

Observación No. 2:

Documento: Proyecto de Pliego de Condiciones.

Página: Página 62 y ss – Numeral 6.2 Criterios para verificación de la experiencia.

Tema: Aceptación de actividades equivalentes para la acreditación de la experiencia habilitante.

Texto del documento: "(...) cuyo objeto o alcance contemple la implementación de soluciones de seguridad informática en entidades estatales o privadas".

Observación y solicitud: Dentro de los requisitos habilitantes de experiencia técnica, la Entidad exige acreditar contratos cuyo objeto o alcance contemple la "implementación de soluciones de seguridad informática en entidades estatales o privadas", teniendo en cuenta que, en el sector de las Tecnologías de la Información y



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

las Comunicaciones (TIC) las actividades técnicas de seguridad informática abarcan diversas denominaciones operativas que conducen al mismo resultado material e idoneidad técnica, resulta indispensable precisar el alcance interpretativo de la expresión "implementación".

Teniendo de presente que en este tipo de procesos debe regir el cumplimiento del principio de Libre Concurrencia y Selección Objetiva que rezan los arts. 2 de la Ley 1150 de 2007 y el art. 24 de la Ley 80 de 1993, además, la jurisprudencia del Consejo de Estado y dentro de los manuales de Colombia Compra Eficiente - CCE se ha establecido de forma reiterada que las reglas sobre experiencia habilitante no deben interpretarse de manera exegética o de literalidad rígida que restrinja la participación de oferentes idóneos.

Por otro lado, debe tenerse en cuenta que la experiencia es la destreza adquirida por la práctica de una actividad determinada, por lo que en contratos de servicios tecnológicos a medida, actividades como despliegue, puesta en marcha, desarrollo, configuración, integración, suministro con instalación y/o prestación de servicios de seguridad informática implican sustancial y técnicamente el mismo esfuerzo operacional y nivel de conocimiento que la "implementación". Y el hecho de exigir de forma taxativa el verbo "implementar" generaría una barrera injustificada a la libre competencia si el alcance ejecutado en los certificados es idéntico o superior.

Por lo anterior, solicitamos amablemente a la entidad confirmar y aclarar qué actividades serán tenidas como válidas y admisibles para la acreditación de la experiencia habilitante, aquellas certificaciones o contratos donde, aun cuando no se utilice taxativamente el verbo rector "implementación", se acredite la ejecución de actividades equivalentes o análogas tales como: Desarrollo, despliegue, puesta en marcha, integración, configuración, administración, aprovisionamiento o prestación de servicios integrales de seguridad informática / ciberseguridad.

Lo anterior, siempre que las actividades descritas en la certificación permitan evidenciar el cumplimiento de la idoneidad técnica en materia de soluciones de seguridad informática requerida por la Entidad.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

La Entidad aclara que, en aras de garantizar la libre concurrencia y la selección objetiva, serán válidas y admisibles aquellas certificaciones de experiencia donde, aun cuando no se utilice taxativamente la palabra "implementación", se certifiquen actividades operativas y técnicas equivalentes o análogas tales como: despliegue, puesta en marcha, integración, configuración, administración, aprovisionamiento o prestación de servicios administrados de seguridad informática / ciberseguridad. Dicha condición aplica siempre y cuando el objeto u obligaciones certificadas permitan verificar la idoneidad técnica en soluciones de seguridad informática.

Observación No. 3

Documento: Proyecto de Pliego de Condiciones.

Página: Página 67 y ss – Numeral 6.4.2. CERTIFICACIONES RELACIONADAS CON EL SOC (CENTRO DE OPERACIONES DE SEGURIDAD) DEL PROPONENTE.

Tema: flexibilización y alternatividad en la exigencia de certificaciones.

Texto del documento: "(...) En relación con el centro de datos donde se encuentra alojado el SOC el cual es objeto de la presente contratación el proponente deberá allegar la siguiente documentación".

Observación y solicitud: En la sección correspondiente a los Requisitos Habilitantes Técnicos / Capacidad Técnica del Pliego de Condiciones, la entidad exige a los proponentes la acreditación obligatoria y acumulativa



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

de cuatro (4) certificaciones relacionadas con el SOC. La obligación de contar simultáneamente con las cuatro certificaciones restringe de manera gravosa la participación en el proceso. Aunque las normas citadas evalúan aspectos complementarios (calidad, seguridad de la información, gestión de servicios TIC y madurez de procesos de software), la exigencia simultánea no es una medida idónea ni indispensable para verificar la idoneidad técnica en el desarrollo de software a medida, por lo que acreditar una o dos de estas certificaciones es suficiente para garantizar la correcta ejecución del contrato, sin necesidad de cerrar el mercado a un grupo reducido de competidores

En la industria de servicios tecnológicos a medida, las empresas adoptan diferentes marcos de trabajo complementados con certificaciones específicas según su nicho de especialización. Forzar la acreditación de la totalidad de la lista limita artificialmente la oferta, perjudicando la eficiencia en el uso de los recursos públicos.

Este tipo de requisitos deben estructurarse de manera objetiva, evitando incluir condiciones desproporcionadas o restrictivas que impidan la libre concurrencia de oferentes capacitados o que otorguen ventajas injustificadas a competidores específicos, ya que con base en el artículo 5 de la Ley 1150 de 2007, modificado por el Artículo 88 de la Ley 1474 de 2011, los requisitos habilitantes deben ser adecuados, necesarios y proporcionales a la naturaleza, cuantía y complejidad del objeto a contratar y el hecho de exigir cuatro certificaciones acumulativas contraviene la proporcionalidad, puesto que la capacidad técnica habilitante puede comprobarse fehacientemente mediante alternativas equivalentes o un número menor de acreditaciones de alto estándar.

Por ello, y con fundamento en las razones expuestas, solicitamos respetuosamente a la Entidad ajustar el Pliego de Condiciones en cualquiera de las siguientes opciones:

- 1. Modificar la redacción para que la acreditación de las certificaciones sea de carácter alternativo y no acumulativo, estableciendo que el proponente cumplirá el requisito habilitante mediante la presentación de al menos una (1) o dos (2) de las certificaciones requeridas (ej. "El proponente deberá acreditar al menos una (1) de las siguientes certificaciones:").*
- 2. Mantener como requisito habilitante obligatorio una (1) certificación principal y trasladar las demás certificaciones al capítulo de Criterios de Ponderación / Puntaje Técnico Opcional, permitiendo que la obtención de certificaciones adicionales otorgue puntaje complementario dentro de la evaluación de la calidad de la oferta.*

RESPUESTA DE LA ENTIDAD: NO SE ACOGE LA SOLICITUD.

La observación parte de una interpretación que no corresponde al requisito establecido por la Entidad.

En efecto, el estudio previo, el numeral 13.3. "CERTIFICACIONES RELACIONADAS CON EL SOC (CENTRO DE OPERACIONES DE SEGURIDAD) DEL PROPONENTE" no establece la obligación de acreditar cuatro (4) certificaciones de manera acumulativa, como lo señala el observante. El requisito contempla diferentes documentos y acreditaciones destinados a verificar condiciones particulares del servicio, entre ellas: la certificación del representante legal respecto de la prestación del servicio en un SOC de propiedad del oferente; la certificación TIER III del Uptime Institute o ICREA Nivel IV del centro de datos donde se encuentra implementado el SOC; y la acreditación como MSSP —Managed Security Service Provider— otorgada por el fabricante del SIEM utilizado para la prestación del servicio.

En consecuencia, no se trata de cuatro certificaciones que puedan ser acreditadas indistintamente por el proponente, ni de certificaciones que tengan una misma finalidad y puedan sustituirse entre sí. Cada una de las



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

condiciones solicitadas permite verificar un aspecto diferente relacionado con la capacidad y condiciones bajo las cuales será prestado el servicio.

Particularmente, la exigencia de contar con un centro de datos certificado bajo TIER III del Uptime Institute o ICREA Nivel IV se encuentra directamente relacionada con las condiciones de infraestructura y disponibilidad requeridas para la operación del SOC. Esta exigencia, además, guarda correspondencia con el Anexo Técnico, que establece que el servicio debe contar con mínimo dos (2) centros de datos ubicados geográficamente en diferentes ciudades y que el centro de datos donde se encuentre alojado físicamente el SOC debe contar con certificación TIER III del Uptime Institute o ICREA Nivel IV.

De igual manera, la acreditación como MSSP por parte del fabricante del SIEM busca verificar una condición específica asociada a la capacidad del proveedor para operar y prestar servicios administrados sobre la tecnología SIEM que será utilizada durante la ejecución contractual, aspecto que no resulta equivalente a la certificación de infraestructura del centro de datos ni puede ser acreditado mediante esta.

Lo anterior resulta especialmente relevante teniendo en cuenta que el objeto contractual comprende la prestación de un servicio integral de SOC, incluyendo el monitoreo y correlación de eventos mediante SIEM, la gestión de incidentes de seguridad y la administración de diferentes componentes de seguridad de la infraestructura tecnológica de la ANM.

Así mismo, el Anexo Técnico establece condiciones de operación continua, seguridad física y lógica, controles de acceso, protección frente a fallas en el suministro de energía y mecanismos de auditoría sobre los procesos, tecnologías y personas que operan el SOC.

En consecuencia, las condiciones exigidas no constituyen requisitos redundantes ni certificaciones intercambiables, sino mecanismos de verificación de aspectos diferenciados y necesarios para garantizar la disponibilidad, seguridad, continuidad y capacidad técnica requerida para la prestación del servicio.

Por lo anterior, la Entidad mantiene el requisito establecido en el Proyecto de Pliego de Condiciones, al considerar que se encuentra directamente relacionado con la naturaleza, complejidad y criticidad del objeto contractual y que su exigencia resulta necesaria para verificar las condiciones mínimas requeridas para la adecuada prestación del servicio de SOC.

De igual manera, se ratifica que la acreditación como MSSP busca verificar la idoneidad y respaldo directo del fabricante de la tecnología SIEM definitiva del contrato (Fortinet). **En consonancia con lo aclarado en la Observación No. 1 de Crossborder Tech, la Entidad modificará el Numeral 6.4.2 del Pliego Definitivo para precisar expresamente que dicha acreditación MSSP debe corresponder al fabricante FORTINET, garantizando la capacidad operativa sobre la plataforma FortiSIEM en la máquina virtual de la Agencia**

Observación No. 4

Tema: Contabilización de la experiencia profesional de los cargos requeridos

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.1 – Experiencia general y experiencia específica

Observación: El Anexo Técnico se establece que se deberá acreditar experiencia general y específica; sin embargo, no precisa el criterio que utilizará la Entidad para contabilizar dicha experiencia. Esta situación puede



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

generar diferentes interpretaciones durante la evaluación de las propuestas, especialmente tratándose de profesiones que pueden requerir matrícula o tarjeta profesional para su ejercicio. Con el fin de garantizar la igualdad entre los proponentes y brindar seguridad jurídica durante la evaluación, resulta conveniente que la Entidad establezca expresamente el criterio de contabilización de la experiencia profesional, de conformidad con el artículo 229 del Decreto Ley 019 de 2012 y la normativa especial que resulte aplicable. Solicitud: Se solicita a la Entidad aclarar expresamente si la experiencia profesional será contabilizada desde la terminación y aprobación del pensum académico, desde la obtención del título profesional o desde la expedición de la matrícula o tarjeta profesional, según corresponda para cada profesión.

RESPUESTA DE LA ENTIDAD: NO SE ACOGE LA OBSERVACIÓN.

De conformidad con lo dispuesto en el artículo 229 del Decreto Ley 019 de 2012 y las normas especiales regulatorias del ejercicio de las ingenierías (Ley 842 de 2003 y afines), la experiencia profesional para las carreras que requieren tarjeta profesional se contabilizará **a partir de la expedición del respectivo documento / matrícula profesional** o de la terminación y aprobación del pensum académico de educación superior, según aplique y esté debidamente certificado por la institución educativa o el consejo profesional correspondiente.

Observaciones No. 5, 6, 8 y 9 (Perfil: Coordinador de Proyecto)

Observación No. 5

Tema: Ampliación de la formación académica exigida para el Coordinador del Proyecto.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.1 – Formación Académica Coordinador de proyecto.

Observación: El perfil limita la formación profesional a determinadas ingenierías y a dos Núcleos Básicos del Conocimiento (NBC). No obstante, actualmente existen otros programas académicos afines que desarrollan competencias equivalentes en dirección de proyectos tecnológicos, infraestructura TI y ciberseguridad, cuyos profesionales pueden desempeñar adecuadamente las funciones requeridas. La ampliación de las profesiones aceptadas no afecta la idoneidad del perfil, toda vez que el requisito de experiencia específica continúa garantizando que el profesional cuente con los conocimientos necesarios para la ejecución del contrato.

Solicitud: Se solicita ampliar las profesiones aceptadas para este perfil, incluyendo programas afines como Ingeniería Informática, Ingeniería de Software, Ingeniería Telemática, Ciencias de la Computación o cualquier otro programa perteneciente a los Núcleos Básicos del Conocimiento relacionados con Tecnologías de la Información y las Comunicaciones registrados en el SNIES.

Observación No. 6

Tema: Flexibilización de las áreas de posgrado exigidas para el Coordinador del Proyecto.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.1 – Posgrado Coordinador de proyecto.

Observación: El Anexo Técnico limita los estudios de posgrado a determinadas áreas del conocimiento. Sin embargo, existen otros programas de especialización, maestría o doctorado que desarrollan competencias directamente relacionadas con la gestión de proyectos tecnológicos y la seguridad de la información, tales como Gobierno de TI, Arquitectura Empresarial, Gestión Tecnológica, Transformación Digital, Ingeniería de Software o Infraestructura Tecnológica. Permitir estas áreas ampliaría la participación de profesionales con formación equivalente sin disminuir el nivel técnico requerido.

Solicitud: Se solicita ampliar las áreas de posgrado aceptadas para este perfil, incluyendo programas relacionados con Gobierno de TI, Arquitectura Empresarial, Gestión Tecnológica, Transformación Digital,



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Gerencia de proyectos, Infraestructura Tecnológica y demás programas afines a las Tecnologías de la Información.

Observación No. 8

Tema: Ampliación del alcance de la experiencia específica del Coordinador del Proyecto.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.1 – Experiencia Específica Coordinador de proyecto.

Observación: El Anexo Técnico exige que el Coordinador del Proyecto acredite experiencia dirigiendo o coordinando proyectos de seguridad de la información. Si bien este requisito guarda relación con el objeto contractual, su alcance resulta restrictivo al excluir profesionales que han liderado proyectos en otras áreas de la ciberseguridad, tales como seguridad informática, seguridad digital, gestión de vulnerabilidades, respuesta a incidentes, operación de SOC, seguridad de redes o gestión de riesgos tecnológicos, las cuales desarrollan competencias igualmente aplicables para la ejecución del contrato.

Solicitud: Se solicita ampliar el requisito de experiencia específica, permitiendo acreditar experiencia en la dirección o coordinación de proyectos relacionados con ciberseguridad, seguridad informática, seguridad digital, operación de SOC, gestión de vulnerabilidades, respuesta a incidentes, gestión de riesgos tecnológicos y demás áreas afines, manteniendo el tiempo mínimo de experiencia exigido por la Entidad.

Observación No. 9

Tema: Coherencia entre el rol solicitado y la experiencia general exigida para el Coordinador del Proyecto.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.1 – Experiencia General Coordinador de proyecto.

Observación: El Anexo Técnico establece que el profesional deberá acreditar una experiencia mínima de cinco (5) años en gerencia o supervisión de proyectos relacionados con seguridad de la información o seguridad informática. Sin embargo, el perfil requerido corresponde al cargo de Coordinador del Proyecto, cuyas funciones no necesariamente implican el desempeño de cargos de gerencia o supervisión.

Esta condición puede restringir la participación de profesionales que han ejercido como coordinadores, líderes técnicos o responsables de la ejecución de proyectos de ciberseguridad, desempeñando funciones acordes con el objeto contractual, sin ostentar formalmente un cargo gerencial. En este sentido, la denominación del cargo no siempre refleja el nivel de responsabilidad asumido dentro de un proyecto.

Solicitud: Se solicita ampliar el requisito de experiencia general, permitiendo acreditar experiencia en coordinación, dirección, liderazgo, administración o supervisión de proyectos relacionados con ciberseguridad, seguridad de la información, seguridad informática o áreas afines, manteniendo el tiempo mínimo de experiencia exigido.

RESPUESTA DE LA ENTIDAD: SE ACOGE PARCIALMENTE Y SE ACLARA.

- **Formación Académica y Posgrado:** La ANM acepta ampliar las titulaciones de pregrado y posgrado a programas pertenecientes al Núcleo Básico del Conocimiento (NBC) en Ingeniería de Sistemas y/o Teleinformática y/o Computación y/o Ciberseguridad y/o Gobierno de TI y/o Gerencia de Proyectos y áreas afines registradas en el SNIES.
- **Experiencia General y Específica:** Se aclara que la experiencia general y específica de cinco (5) años podrá certificarse en actividades de *coordinación, dirección, gerencia, liderazgo técnico o supervisión* de proyectos de seguridad de la información, ciberseguridad, ciberdefensa o gestión de riesgos tecnológicos.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observación No. 7

Tema: Flexibilización de las certificaciones internacionales exigidas para el Coordinador del Proyecto.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.1 – Certificaciones Coordinador de proyecto.

Observación: El requisito establece un listado específico de certificaciones internacionales para acreditar las competencias del Coordinador del Proyecto. Aunque dichas certificaciones son ampliamente reconocidas, existen otras credenciales expedidas por organismos internacionales que acreditan competencias equivalentes en gestión de seguridad, gobierno de TI, continuidad del negocio y gestión de riesgos. Limitar el cumplimiento del requisito a un listado cerrado reduce la pluralidad de oferentes, aun cuando existan certificaciones de igual reconocimiento internacional.

Solicitud: Se solicita aceptar certificaciones internacionales equivalentes, tales como ISO/IEC 27001 Lead Implementer, ISO/IEC 27032 Lead Cybersecurity Manager, Lead Manager NIST Cybersecurity Framework 2.0 (PECB), CompTIA Security+, GIAC Security Essentials (GSEC) cualquier otra certificación que acredite competencias equivalentes en gestión de la seguridad de la información.

RESPUESTA DE LA ENTIDAD: SE ACOGE PARCIALMENTE Y SE ACLARA

De conformidad con el artículo 5 de la Ley 1150 de 2007 y las directrices emitidas por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente (CCE), los requisitos habilitantes deben ser proporcionales, necesarios y no deben imponer barreras de entrada mediante la exigencia obligatoria de certificaciones privadas específicas (como las normas de la familia ISO) cuando estas no estén dictadas por un reglamento técnico obligatorio nacional.

Exigir de manera mandatoria o restringir el cumplimiento a certificaciones bajo estándares ISO específicas para el personal podría vulnerar los principios de libre competencia e igualdad de condiciones entre los oferentes.

Por lo que, en atención a los principios de selección objetiva, proporcionalidad y pluralidad de oferentes, la Agencia Nacional de Minería acepta e incorpora dentro del abanico de certificaciones válidas para el perfil del Coordinador del Proyecto las credenciales internacionales orientadas a la gestión y gobierno de la seguridad de la información, tales como: CompTIA Security+, GIAC Security Essentials (GSEC), Lead Manager NIST Cybersecurity Framework.

Se reitera que el profesional propuesto deberá acreditar mínimo una (1) certificación internacional vigente dentro del listado ampliado en los Pliegos Definitivos, manteniendo de manera paralela los requisitos de formación académica (pregrado/posgrado) y los 5 años de experiencia general y específica exigidos para el cargo.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observaciones No. 10, 11, 12, 13 y 14 (Perfil: Profesional Senior de Redes y Seguridad Informática)

Observación No. 10

Tema: Ampliación de la formación académica del Profesional Senior de Redes y Seguridad Informática.

Información pública



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.2 – Profesional Senior Redes y Seguridad Informática – Formación Académica.

Observación: El perfil limita la formación profesional a determinadas ingenierías y a dos Núcleos Básicos del Conocimiento (NBC). No obstante, existen otros programas académicos afines que desarrollan competencias equivalentes para el diseño, administración y operación de infraestructuras tecnológicas y soluciones de ciberseguridad.

La ampliación de la formación académica permitiría la participación de profesionales con conocimientos y experiencia equivalentes, sin afectar la idoneidad técnica del perfil requerido, toda vez que la experiencia específica y las certificaciones continúan garantizando las competencias necesarias para la ejecución del contrato.

Solicitud: Se solicita ampliar las profesiones aceptadas para este perfil, incluyendo títulos profesionales pertenecientes a otros Núcleos Básicos del Conocimiento relacionados con Tecnologías de la Información y las Comunicaciones, tales como Ingeniería Informática, Ingeniería de Software, Ciencias de la Computación, Ingeniería en Ciberseguridad o programas afines registrados en el SNIES.

Observación No. 11

Tema: Flexibilización del número mínimo de certificaciones exigidas, profesional senior redes y seguridad informática.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.2 – Certificaciones de Profesional senior redes y seguridad informática.

Observación: El perfil exige acreditar como requisito habilitante al menos dos (2) certificaciones internacionales vigentes. Si bien las certificaciones constituyen un mecanismo válido para acreditar conocimientos especializados, la exigencia de múltiples certificaciones, sumada a la experiencia general y específica requerida, restringe considerablemente la disponibilidad de profesionales en el mercado.

La experiencia profesional y la trayectoria en proyectos de seguridad informática también constituyen mecanismos idóneos para demostrar competencias técnicas, por lo que mantener un número elevado de certificaciones podría limitar la pluralidad de oferentes. Solicitud: Se solicita reducir el requisito a una (1) certificación internacional vigente o, alternativamente, permitir que una de las certificaciones pueda ser homologada mediante experiencia específica adicional debidamente certificada.

Observación No. 12

Tema: Flexibilización de las certificaciones Profesional Senior de Redes y Seguridad Informática.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.2 – Certificaciones y Experiencia Específica.

Observación: El Anexo Técnico exige certificaciones específicas de organismos como ISACA y Fortinet, así como experiencia exclusiva en tecnologías de este fabricante. Si bien estos requisitos guardan relación con el objeto contractual, existen certificaciones y soluciones tecnológicas equivalentes ampliamente reconocidas en el mercado que acreditan competencias similares en seguridad de la información, gestión de riesgos, auditoría y administración de plataformas de ciberseguridad. Limitar las certificaciones y la experiencia a un fabricante u organismo específico reduce la pluralidad de oferentes, sin que ello represente necesariamente un mayor nivel técnico para la ejecución del contrato.

Solicitud: Se solicita permitir la acreditación de certificaciones y experiencia mediante tecnologías y credenciales equivalentes, tales como CISSP, SSCP, ISO/IEC 27001 Lead Auditor, ISO/IEC 27001 Lead Implementer, CompTIA Security+, FCP Security, FCSS Security, así como certificaciones equivalentes de fabricantes como Palo Alto, Check Point, Cisco, Sophos o Juniper, siempre que acrediten competencias similares a las exigidas en el presente proceso. Asimismo, se solicita aceptar experiencia en la administración de soluciones de seguridad equivalentes, manteniendo el nivel técnico requerido para el perfil.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Observación No. 13

Tema: Ampliación de la experiencia específica en el Profesional senior redes y seguridad informática.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.2 – Experiencia Específica.

Observación: El requisito limita la experiencia a productos específicos del fabricante Fortinet FORTINET – WAF – ANALIZER – FORTIGATE., ZTNA, dejando por fuera otras tecnologías ampliamente utilizadas en proyectos de ciberseguridad, como plataformas SIEM, EDR, XDR, NAC, CASB, PAM o soluciones de protección perimetral y de identidad. Considerando que el objeto contractual corresponde a servicios de ciberseguridad, resulta conveniente valorar la experiencia funcional en tecnologías de seguridad y no únicamente la experiencia en un fabricante específico.

Solicitud: Se solicita ampliar el requisito de experiencia específica para aceptar experiencia en implementación, administración u operación de soluciones NGFW, WAF, SIEM, EDR, XDR, ZTNA, PAM, CASB, NAC, IAM y demás tecnologías de seguridad equivalentes, independientemente del fabricante.

Observación No. 14.

Tema: Homologación entre certificaciones y experiencia específica.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.2 – Certificaciones Profesional senior redes y seguridad informática.

Observación: El perfil permite acreditar la formación académica y la experiencia; sin embargo, no contempla la posibilidad de homologar parcialmente el requisito de certificaciones mediante experiencia adicional. En el mercado existen profesionales con amplia trayectoria administrando plataformas de seguridad que, si bien no cuentan con múltiples certificaciones vigentes, poseen conocimientos demostrables adquiridos durante años de experiencia en proyectos similares. Permitir una homologación parcial incrementa la pluralidad de oferentes sin afectar la capacidad técnica del recurso humano.

Solicitud: Se solicita evaluar la posibilidad de permitir que una (1) de las certificaciones exigidas pueda homologarse mediante dos (2) años adicionales de experiencia específica en administración de plataformas de seguridad informática, debidamente certificada.

RESPUESTA DE LA ENTIDAD:

Luego de analizar las observaciones presentadas, así como el perfil requerido, se señala lo siguiente:

- **Formación Académica:** Se aceptan titulaciones en el NBC de Ingeniería de Sistemas, y/o Electrónica, y/o Telecomunicaciones, y/o Ciberseguridad o afines SNIES.
- **Certificaciones y Experiencia Específica (Fortinet):** Dado que el objeto contractual implica la administración directa y configuración de los equipos perimetrales propiedad de la ANM (NGFW FortiGate, FortiWeb, FortiAnalyzer y ZTNA), es **indispensable** que el Profesional Senior cuente con la certificación mandatoria en el ecosistema Fortinet (Fortinet Certified Associate/Professional/Expert o equivalente NSE 4+) y experiencia específica en dicha tecnología. Por tanto, no se acepta reducir el número de certificaciones ni eliminar la exigencia en la marca de la infraestructura perimetral a administrar.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observaciones No. 15, 16, 17, 18 y 19 (Perfil: Analista de Ciberseguridad)



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Observación No. 15

Tema: Ampliación de la formación académica del Analista de Ciberseguridad.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.3 – Formación Académica.

Observación: El perfil limita la formación profesional a determinadas ingenierías y a dos Núcleos Básicos del Conocimiento (NBC). Sin embargo, existen otros programas académicos afines que forman profesionales con competencias en seguridad informática, infraestructura tecnológica, desarrollo de software y administración de plataformas tecnológicas, las cuales resultan pertinentes para el objeto contractual.

Solicitud: Se solicita ampliar las profesiones aceptadas para este perfil, permitiendo la participación de profesionales pertenecientes a otros Núcleos Básicos del Conocimiento relacionados con Tecnologías de la Información y las Comunicaciones, tales como Ingeniería Informática, Ingeniería de Software, Ciencias de la Computación, Ingeniería en Ciberseguridad y demás programas afines registrados en el SNIES.

Observación No. 16

Tema: Flexibilización de las áreas de posgrado exigidas para el Analista de Ciberseguridad.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.3 – Posgrado.

Observación: El requisito limita los estudios de posgrado a áreas específicas relacionadas con seguridad informática y auditoría de sistemas. No obstante, en el Sistema Nacional de Información de la Educación Superior (SNIES) existen programas de especialización y maestría registrados con diferentes denominaciones, pero pertenecientes a los mismos campos de conocimiento y con competencias equivalentes para el desempeño del cargo, tales como Gobierno de TI, Gestión Tecnológica, Gestión de Riesgos Tecnológicos, Arquitectura Empresarial, Infraestructura Tecnológica y Transformación Digital.

Solicitud: Se solicita ampliar las áreas de posgrado aceptadas, incluyendo programas afines registrados en el SNIES dentro de los campos relacionados con Tecnologías de la Información, gestión tecnológica, gobierno de TI, infraestructura tecnológica y gestión de riesgos, manteniendo el nivel académico exigido y permitiendo la participación de profesionales con formación equivalente.

Observación No. 17

Tema: Flexibilización del número mínimo de certificaciones exigidas para Analista de ciberseguridad.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.3 – Certificaciones.

Observación: El perfil exige acreditar como requisito habilitante tres (3) certificaciones internacionales vigentes. Considerando que el perfil también exige formación profesional, estudios de posgrado y cinco (5) años de experiencia, la exigencia de tres certificaciones puede restringir la participación de profesionales que cuentan con amplia experiencia formación especializada, pero no poseen múltiples certificaciones vigentes.

Solicitud: Se solicita reducir el requisito a dos (2) certificaciones internacionales o permitir que una de ellas pueda homologarse mediante experiencia específica adicional debidamente certificada.

Observación No. 18

Tema: Ampliación del alcance de la experiencia específica para Analista de ciberseguridad.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.3 – Experiencia Específica.

Observación: El perfil exige experiencia mínima en seguridad de la información o seguridad informática. Si bien estas áreas son pertinentes, actualmente la ciberseguridad comprende un espectro más amplio de actividades técnicas, como operación de centros de operaciones de seguridad (SOC), respuesta a incidentes, gestión de



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

vulnerabilidades, seguridad en la nube, ciberdefensa, seguridad de redes y protección de infraestructuras críticas. Ampliar el alcance de la experiencia permitiría la participación de profesionales con trayectoria en áreas directamente relacionadas con el objeto contractual.

Solicitud: Se solicita permitir que la experiencia específica pueda acreditarse en actividades relacionadas con ciberseguridad, seguridad digital, operación de SOC, respuesta a incidentes, gestión de vulnerabilidades, ciberdefensa, seguridad en redes, seguridad en la nube y demás áreas afines, manteniendo el tiempo mínimo de experiencia exigido.

Observación No. 19

Tema: Homologación entre certificaciones y experiencia específica para analista de ciberseguridad.

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Numeral: 4.3 – Certificaciones.

Observación: El Anexo Técnico contempla la homologación entre el posgrado y la experiencia profesional; sin embargo, no prevé una alternativa similar para el requisito de certificaciones internacionales. Considerando que existen profesionales con amplia experiencia en ciberseguridad y operación de plataformas de seguridad, una homologación parcial contribuiría a ampliar la pluralidad de oferentes sin afectar la calidad técnica del perfil.

Solicitud:

Se solicita evaluar la posibilidad de permitir que las certificaciones exigidas puedan homologarse mediante experiencia específica adicional debidamente certificada en actividades relacionadas con ciberseguridad, seguridad informática o seguridad digital.

RESPUESTA DE LA ENTIDAD: SE ACOGE PARCIALMENTE Y SE ACLARA.

- **Formación y Posgrados:** Se amplía la aceptación a programas académicos en Ingeniería de Sistemas, y/o Telecomunicaciones, y/o Ciberseguridad, y/o Auditoría, y/o Riesgo Tecnológico y áreas afines registradas en el SNIES.
- **Experiencia Específica:** Se aclara que la experiencia específica de cinco (5) años se entenderá válida en actividades de seguridad informática, ciberseguridad, respuesta a incidentes, gestión de vulnerabilidades o ciberdefensa.
- **Certificaciones:** Se mantendrá la exigencia de las certificaciones requeridas debido a la diversidad de dominios de análisis que debe cubrir este rol en el SOC.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observación No. 20

Observación No. 20.

Documento: Borrador Clausulado Complementario.

Página / Numeral: Cláusula Quinta (Forma de Pago).

Tema: Forma de pago para el licenciamiento y adquisición de productos.

Observación y solicitud: El clausulado y los estudios previos prevén un esquema de facturación mensual vencida para la totalidad de los bienes y servicios del contrato. Sin embargo, las soluciones de software y renovaciones de licenciamiento de los fabricantes (como la renovación de licenciamientos Fortinet, Vicarius VRX y la adquisición de FortiPAM) se comercializan en el mercado mayorista de distribución tecnológica bajo la modalidad de pago anual anticipado (Lump Sum), siendo imposible que los integradores o canales oficiales



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

de distribución mensualicen el pago del costo de fábrica de estas licencias. Exigir este esquema de pagos mensualizados atenta contra la viabilidad económica y la liquidez de los oferentes.

Por lo anterior, se solicita amablemente a la entidad modificar la Cláusula Quinta (Forma de Pago) para que se estipule expresamente que la adquisición de licencias y las renovaciones de soporte de fábrica (como Vicarius, FortiPAM y licenciamiento perimetral Fortinet) se cancelen en un único pago (Lump Sum) vencido, una vez el contratista entregue a satisfacción la certificación de activación de las licencias y el respectivo soporte directo expedido por el fabricante a nombre de la ANM.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE MODIFICA EL CLAUSULADO.

La Agencia Nacional de Minería reconoce la dinámica operativa del mercado mayorista de software y licenciamiento de ciberseguridad, donde los fabricantes e integradores comercializan y activan las suscripciones de soporte y uso de herramientas en esquemas de pago anual. Por lo tanto, exigir una mensualización sobre la adquisición del licenciamiento afectaría la liquidez y la viabilidad financiera del contrato.

La Entidad modificará la **Forma de Pago** en los estudios previos, así como en la Minuta del Contrato, estableciendo la diferenciación en las modalidades de pago de la siguiente manera:

1. **Licenciamiento y Adquisición de Productos (Ítems 6, 7, 8 y 9 / Fortinet, Vicarius VRX, FortiSIEM VM y FortiPAM):**

Se cancelarán en **un único pago**, una vez el contratista entregue a entera satisfacción de la supervisión del contrato la certificación oficial de activación de las licencias y/o soporte directo expedido por el respectivo fabricante a nombre de la Agencia Nacional de Minería, acompañado de la respectiva acta de recibo a satisfacción.

2. **Servicios Administrados, Monitoreo y Pruebas (Ítems 1, 2, 3, 4 y 5 / Operación SOC, Monitoreo Defender, Administración PAM, Pruebas de Seguridad y SIEM SaaS Transitorio):**

Se mantendrán bajo la modalidad de **pagos mensualizados vencidos**, previa presentación del informe mensual de ejecución, verificación del cumplimiento de los Acuerdos de Niveles de Servicio (ANS) y aprobación del supervisor.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observación No. 21

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 7.1.

Tema: Dimensionamiento y discrepancia de capacidad (EPS) de la solución SIEM temporal vs local.

Observación y solicitud: El Anexo Técnico establece en el Literal 7.2 que el proveedor debe prestar el servicio correlacionador de eventos SIEM en la modalidad de software como servicio (SaaS) durante los primeros dos (2) meses de ejecución con una capacidad máxima de 512 EPS. No obstante, el ítem definitivo a adquirir y configurar localmente es una solución virtualizada FortiSIEM propia de la ANM con capacidad para cincuenta (50) dispositivos y mil (1000) EPS. Limitar la fase de transición temporal a solo 512 EPS pone en riesgo la



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

recolección integral de logs e impide la correcta correlación cruzada de las 10 fuentes mínimas obligatorias detalladas en el mismo Literal, lo cual generaría brechas de monitoreo durante los primeros meses.

Se solicita por ello, unificar y dimensionar la capacidad de la fase temporal SIEM SaaS (meses 1 y 2) para que cuente con soporte de hasta mil (1000) EPS, garantizando que el diseño y el dimensionamiento de las reglas de correlación mantengan consistencia técnica idéntica con la solución FortiSIEM definitiva.

RESPUESTA DE LA ENTIDAD: NO SE ACOGE LA SOLICITUD.

La capacidad de 512 EPS filtrados definida para el servicio SaaS de transición durante los primeros dos (2) meses es técnicamente suficiente para realizar la ingesta y correlación de las fuentes críticas principales durante la fase de empalme y estabilización. La solución definitiva en VM (FortiSIEM) contará con el licenciamiento contratado de 1.000 EPS para el despliegue total de la infraestructura propia.

Observación No. 22

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 4.2.

Tema: Dedicación presencial del Profesional Senior de Redes y Seguridad Informática.

Observación y solicitud: El literal exige que el Profesional Senior de Redes y Seguridad Informática tenga dedicación completa en sitio y sea el canal directo de comunicación entre el personal asignado por la ANM en horario 5x8. No obstante, la Cláusula Vigésima Séptima (Sede del Servicio / Parágrafo 1) de la minuta señala de manera expresa que este servicio de SOC y la administración de plataformas perimetrales se pueden prestar de forma remota desde las instalaciones del contratista, coordinando asistencias presenciales conforme la necesidad de la ANM. Exigir la presencia obligatoria 100% en sitio contradice el modelo remoto del SOC y genera sobrecostos operativos innecesarios.

Se solicita por ello, aclarar y armonizar los términos para permitir expresamente que el Profesional Senior de Redes y Seguridad Informática preste sus servicios de forma remota desde el SOC del contratista, comprometiéndose a realizar asistencias presenciales obligatorias en la Sede Central en Bogotá previa coordinación conjunta y cuando las necesidades operativas de la supervisión lo requieran.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

La ANM aclara que la prestación de los servicios de monitoreo y administración se realiza de manera remota a través del SOC del contratista. Por lo tanto, se precisa que la dedicación del Profesional Senior de Redes y Seguridad Informática operará en modalidad remota (horario 5x8), requiriéndose su presencia física en la Sede Central de la ANM en Bogotá previa solicitud o coordinación con la supervisión contractual cuando las actividades técnicas o la atención de incidentes lo ameriten.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observación No. 23

Documento: Proyecto de Pliego de Condiciones - Requisitos Técnicos Habilitantes (SOC).

Página / Numeral: 36 y ss.

Tema: Forma de pago para el licenciamiento y adquisición de productos.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Observación y solicitud: El pliego exige que el oferente cuente con un Centro de Operaciones de Seguridad (SOC) propio y que el centro de datos donde se encuentra alojado físicamente cuente con certificación TIER III de Uptime Institute o ICREA Nivel IV. En el mercado nacional, las oficinas de trabajo y monitoreo desde donde operan físicamente los analistas del SOC son áreas administrativas estándar que consumen software de monitoreo basado en la nube, mientras que el motor centralizado del SIEM se aloja en nubes públicas (como AWS, Azure o Google) o data centers externos certificados. Exigir que toda la infraestructura física de las oficinas de analistas del proponente posea certificación TIER III es restrictivo y carece de sustento técnico. Se solicita por ello, aclarar y certificar en el pliego que la certificación TIER III de Uptime Institute o ICREA Nivel IV aplica de manera exclusiva para la infraestructura del centro de datos principal o secundario donde se encuentra alojado el core físico o virtual del SIEM/SOC y no a las oficinas de trabajo administrativo del personal de análisis.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

La Entidad aclara que la exigencia de certificación TIER III (Uptime Institute) o ICREA Nivel IV **aplica de manera exclusiva para el Data Center** donde se encuentra alojada la infraestructura central, servidores y el core del SOC del proponente. No se requiere dicha certificación para las estaciones de trabajo u oficinas administrativas desde donde interactúan los analistas de seguridad.

Observación No. 24.

Documento: Proyecto de Pliego de Condiciones - Requisitos Técnicos Habilitantes (SOC).

Página / Numeral: 67.

Tema: Exigencia de reportes SOC 2 o SOC 3 vigente del proponente.

Observación y solicitud: El pliego exige que el oferente cuente con un reporte SOC 2 o SOC 3 vigente sobre sus servicios de ciberseguridad y ciberdefensa. En Colombia, el reporte SOC (System and Organization Controls) es una de las normas de auditoría de origen estadounidense (emitida bajo estándares de la AICPA) de muy alto costo y de escasa aplicación para empresas de tecnología locales, las cuales en su lugar estandarizan y auditan sus procesos bajo la norma internacional ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información) e ISO/IEC 20000-1 (Gestión de Servicios de TI). Solicitar reportes SOC 2/SOC 3 limita gravemente la participación de la industria nacional.

Se solicita amablemente a la entidad permitir la homologación del reporte SOC 2 o SOC 3, aceptando de manera alternativa que el proponente acredite contar con certificación internacional vigente bajo las normas ISO/IEC 27001:2013 o ISO/IEC 27001:2022 para el alcance de Servicios de Centro de Operaciones de Seguridad (SOC) o Monitoreo de Ciberseguridad.

RESPUESTA DE LA ENTIDAD: NO SE ACOGE LA SOLICITUD.

El reporte de atestación **SOC 2 / SOC 3** evalúa operacionalmente los controles de seguridad, disponibilidad, confidencialidad y privacidad del servicio prestado por el proveedor, constituyendo una garantía objetiva sobre la efectividad de la operación del SOC. Por lo tanto, la Entidad mantiene este requisito para verificar la madurez operativa del Centro de Operaciones ofertado

Observación No. 25

Documento: Anexo Técnico – Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 7.5.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Tema: Alcance del Re-Test de Vulnerabilidades técnicas.

Observación y solicitud: El pliego establece que el contratista realizará una prueba de vulnerabilidad para un mínimo de cien (100) direcciones IP y, posteriormente, un Re-Test a los seis (6) meses de ejecución. No obstante, se señala que para el Re-Test la ANM podrá cambiar hasta el 100% de las direcciones IP analizadas en la primera prueba. Técnicamente, un ejercicio de 'Re-Test' consiste en re-escanear y validar de manera exclusiva si los hallazgos críticos e importantes encontrados en el primer análisis sobre las mismas IPs fueron correctamente remediados y mitigados. Modificar las IPs al 100% desnaturaliza el concepto técnico de Re-Test, convirtiéndolo en un segundo escaneo inicial sin línea base de remediación.

Se solicita por ello aclarar que el Re-Test a ejecutarse a los seis (6) meses de vigencia se limitará estrictamente al alcance y a las mismas cien (100) direcciones IP del análisis inicial, para asegurar la correcta validación y el cálculo del progreso de mitigación de la línea base original.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

Se aclara al observante que el objetivo técnico del Re-Test es la validación y verificación del estado de remediación de las vulnerabilidades identificadas en la línea base inicial. Por ende, el Re-Test semestral se ejecutará sobre el mismo segmento de **100 direcciones IP analizadas en la primera prueba**. De requerirse la inclusión de nuevas IPs por cambios en la infraestructura, esto se coordinará previamente con la supervisión sin exceder el tope contratado.

Observación No. 26:

Documento: Proyecto de Pliego de Condiciones - Requisitos Técnicos Habilitantes (auditoría).

Tema: Exigencia de Auditoría de Madurez de Operaciones de Seguridad (SOMM).

Observación y solicitud: El pliego de condiciones establece que las tecnologías, procesos y personas que operan el SOC del proponente deben haber sido auditados por un ente externo bajo el modelo de madurez de operaciones de seguridad (SOMM - Security Operations Maturity Model) al menos una vez en los últimos tres (3) años. El modelo SOMM es un marco metodológico conceptual interno de análisis y no existe en Colombia una entidad o ente acreditador formalmente constituido y reconocido por el ONAC que emita 'certificaciones oficiales' de madurez SOMM. Exigir este requisito con carácter obligatorio inhabilita de plano al mercado de ciberseguridad nacional de forma injustificada.

Se solicita por ello amablemente, suprimir la exigencia obligatoria de contar con una auditoría externa bajo el modelo de madurez SOMM o, en su defecto, permitir que dicha madurez sea acreditada mediante una autoevaluación firmada por el Oficial de Seguridad del proponente o mediante certificaciones internacionales de sus analistas principales (como GIAC, Certified SOC Analyst, CISSP).

RESPUESTA DE LA ENTIDAD: NO SE ACOGE LA SOLICITUD DE SUPRIMIR.

La Entidad mantiene la exigencia de verificar la madurez del SOC mediante el modelo SOMM o metodologías equivalentes de medición de madurez de operaciones de ciberseguridad. Sin embargo, se aclara que la auditoría de madurez puede ser emitida por un tercero auditor independiente o una firma consultora externa especializada que haya evaluado los procesos, personas y tecnologías del SOC dentro del periodo fijado en los pliegos.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observación No. 27



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Documento: Anexo Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 7.1.

Tema: Deslinde de responsabilidades y ANS en administración de WAF por terceros.

Observación y solicitud: El Literal 7.1 señala en una nota de aclaración que la administración física de los dispositivos WAF (Firewall de Aplicaciones Web) ubicados en el Datacenter Principal de la ANM corresponde a un tercero ajeno a esta contratación, por lo que el contratista solo coordinará cambios. Dado que el contratista no tiene el acceso lógico directo ni la potestad física de aplicar los cambios de manera directa y autónoma, dependerá exclusivamente de la agilidad y respuesta del tercero para cumplir con los Acuerdos de Niveles de Servicio (ANS).

Se solicita establecer expresamente en el pliego y en el clausulado que el contratista estará eximido de cualquier descuento, multa o incumplimiento de niveles de servicio (ANS) originados por demoras, fallas o falta de respuesta del tercero encargado de la administración directa de los dispositivos WAF en el Datacenter de la ANM.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

La ANM confirma que el contratista no será sancionado ni sujeto a deducciones sobre los Acuerdos de Niveles de Servicio (ANS) cuando los retrasos, indisponibilidades o fallas sean causadas de forma comprobada por la falta de respuesta, demoras en la ventana de mantenimiento o la gestión directa del tercero a cargo de la administración física de los WAF. El contratista deberá dejar constancia documental de las solicitudes de cambio y tiempos de escalamiento presentados a dicho tercero.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observación No. 28.

Documento: Anexo Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 7.7.

Tema: Información técnica de equipos Fortinet a renovar (Serial Numbers).

Observación y solicitud: El cuadro de licenciamientos Fortinet a renovar detalla los modelos (2 NGFW FG-1100E, 2 FortiWeb 1000E, 1 FortiAnalyzer 300G, etc.). Para que los proponentes puedan realizar el dimensionamiento exacto y cotizar ante el canal oficial de Fortinet en Colombia sin incurrir en imprecisiones o sobrecostos técnicos de fábrica (como recargos por expiración o discrepancias de modelos exactos), se requiere contar con la certeza absoluta del inventario detallado de la infraestructura a cotizar. Se solicita amablemente a la entidad confirmar de manera definitiva y oficial a través de una tabla consolidada dentro de los pliegos o mediante una adenda los números de serie (Serial Numbers) exactos y el estado actual de las suscripciones de cada uno de los dispositivos perimetrales objeto de la renovación de licenciamiento para evitar errores de cotización de fábrica.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD.

La Agencia Nacional de Minería publicará dentro del Anexo de Especificaciones y Requerimientos Mínimos Definitivo los **números de serie (Serial Numbers)** de los 2 NGFW FortiGate 1100E, 2 FortiWeb 1000E, 1 FortiAnalyzer 300G y las suscripciones ZTNA para la correcta validación ante el canal oficial de Fortinet.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observación No. 29:

Documento: Anexo Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 7.1 (Soporte Sentinel).

Tema: Exclusión de costos de consumo e ingesta en Microsoft Sentinel.

Observación y solicitud: El pliego requiere la configuración y monitoreo de alertas procedentes de la plataforma Microsoft Sentinel de la ANM. Técnicamente, Microsoft Sentinel es un SIEM nativo en la nube (SaaS sobre Azure) cuyos costos de operación están asociados directamente a la cantidad de gigabytes de datos ingeridos por día y al tiempo de retención de logs en la nube. Un aumento abrupto en la ingesta de fuentes de red podría generar cobros variables extremadamente elevados en la cuenta de Azure de la entidad.

Se solicita amablemente confirmar de manera expresa que la ANM asumirá el 100% de los costos de licenciamiento, ingesta, almacenamiento, retención de logs y consumos en la nube de Azure de su plataforma Microsoft Sentinel, limitándose el contratista de forma exclusiva a aportar los analistas para la gestión lógica y configuración de reglas de correlación.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La Entidad ACLARA que la plataforma Microsoft Sentinel. no ha sido implementada en la ANM y una vez implementado por parte de la ANM, por lo que se ACLARA que el alcance del contratista se limita al monitoreo, análisis, correlación y gestión de incidentes por parte de los analistas del SOC.

Observación No. 30.

Documento: Borrador Clausulado Complementario.

Página / Numeral: Cláusula Vigésima Primera (Liquidación).

Tema: Inconsistencia en el plazo de liquidación bilateral del contrato.

Observación y solicitud: Existe una contradicción directa entre los Estudios Previos y la minuta complementaria del contrato. En el documento de Estudios Previos (numeral 20) se establece de manera clara que el contrato se liquidará en forma bilateral dentro de los seis (6) meses siguientes a su terminación. Sin embargo, en el Borrador Clausulado Complementario (Cláusula Vigésima Primera) se estipula de forma mandatoria que la liquidación bilateral deberá realizarse dentro de los cuatro (4) meses siguientes a la finalización. Esto genera incertidumbre jurídica para el cierre administrativo del proceso.

Se solicita por ello, unificar los términos y estipular en ambos documentos que el contrato se liquidará bilateralmente dentro de los cuatro (4) meses siguientes a su terminación, conforme al término estándar de eficiencia administrativa establecido en la Ley 1150 de 2007.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD.

La Entidad unifica los términos en los documentos del proceso, estableciendo que el plazo para la **liquidación bilateral del contrato será de cuatro (4) meses** contados a partir de su terminación, de conformidad con lo previsto en el artículo 11 de la Ley 1150 de 2007.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Observación No. 31.

Documento: Anexo Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 7.5.

Tema: Ambigüedad en la cantidad de usuarios para prueba de ingeniería social.

Observación y solicitud: En diferentes partes del Anexo Técnico se evidencian inconsistencias respecto al número de usuarios a impactar con la prueba de ingeniería social y simulación de phishing. El Literal 7.5 en un fragmento menciona que la simulación debe dirigirse a la totalidad de cuentas de correo, estimando aproximadamente 1850 usuarios. Sin embargo, en el mismo numeral se detallan 1750 usuarios y, en el cuadro de monitoreo de Defender, se mencionan 1750 buzones y 1200 estaciones. Para cotizar de manera precisa el licenciamiento de la simulación de phishing, los oferentes requieren conocer el alcance exacto.

Se solicita por ello, unificar y aclarar cuál es la cantidad exacta de buzones y usuarios finales que conformarán el alcance definitivo del licenciamiento y de la ejecución de la prueba de ingeniería social y simulación de phishing de este contrato.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La Entidad precisa que el alcance definitivo para el dimensionamiento de la prueba de ingeniería social y simulación de phishing corresponde a un universo de **hasta 1.850 usuarios / buzones corporativos** de la Agencia Nacional de Minería.

Observación No. 32

Documento: Anexo Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Lugar de Ejecución.

Tema: Cobertura geográfica de viáticos y desplazamientos para regionales.

Observación y solicitud: El anexo señala que el proponente debe asumir la totalidad de costos asociados a logística, desplazamientos y viáticos para atender los soportes de la ANM. Sin embargo, los estudios previos mencionan que la ANM cuenta con once (11) Puntos de Atención Regional, Estaciones de Salvamento Minero y sedes de apoyo a nivel nacional en diferentes departamentos de Colombia. Obligar al proponente a asumir de manera indefinida los viáticos por visitas físicas de soporte a todas las regionales rompe el equilibrio económico de la oferta.

Se solicita aclarar que el soporte presencial de ingeniería se limitará de forma exclusiva a la Sede Central en la ciudad de Bogotá, y que el soporte para las once (11) regionales y estaciones de salvamento de la ANM se prestará de manera 100% remota o que, en caso de requerirse soporte físico in situ en las regionales aprobado por el supervisor, la ANM cubrirá la totalidad de viáticos de viaje del personal.

RESPUESTA DE LA ENTIDAD:

Se aclara al oferente que el soporte e ingeniería presencial exigidos aplican **exclusivamente para la Sede Central de la ANM en la ciudad de Bogotá D.C.** El soporte técnico para las Puntos de Atención Regional (PAR) y Estaciones de Salvamento Minero se prestará de forma **100% remota**. En el evento excepcional de requerirse un desplazamiento presencial a alguna sede regional por orden previa y justificada de la supervisión, los gastos de viáticos y transporte deberán ser asumidos por el contratista.

Observación No. 33



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Documento: Borrador Clausulado Complementario.

Página / Numeral: Cláusula Cuarta (CDP y Regalías SGR).

Tema: Protección ante retrasos administrativos en los giros del Sistema General de Regalías (SGR).

Observación y solicitud: El presupuesto del contrato se encuentra respaldado por una financiación mixta, incluyendo \$140.000.000 COP provenientes del Sistema General de Regalías (SGR - CDP 5426) administrado bajo la plataforma SPGR. Los giros y trámites de desembolso del SGR conllevan procesos de revisión externos a la ANM que históricamente suelen presentar retrasos administrativos considerables de pago ajenos al contratista, lo cual podría ahogar financieramente al proveedor si se le exige sostener la operación del SOC 7x24x365 sin recibir los pagos.

Se solicita estipular una cláusula de salvaguarda en el contrato que determine que en caso de presentarse demoras administrativas de desembolso de los recursos respaldados por el SGR (CDP 5426), el contratista no será penalizado con multas ni se le declarará incumplimiento de niveles de servicio (ANS), y que se dará prioridad al pago oportuno utilizando los recursos de inversión del PGN (CDP 89426) disponibles.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La Entidad adelanta las gestiones administrativas de acuerdo con la normatividad del Sistema General de Regalías (SGR) para garantizar el flujo de recursos. Los trámites de pago están sujetos a los procedimientos de ley y al Plan Anualizado de Caja – PAC establecido por el Ministerio de Hacienda y Crédito Público. Así mismo, se ACLARA que no es posible realizar priorización de los recursos del Presupuesto General de la Nación – PGN, por cuanto, en principio se debe mantener la proporcionalidad de los recursos

Observación No. 34

Documento: Anexo Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 7.5.

Tema: Suministro de entornos de preproducción para la prueba de Ethical Hacking.

Observación y solicitud: El Anexo Técnico establece la obligación de realizar pruebas de Ethical Hacking o penetración sobre diez (10) portales públicos de la ANM. No obstante, para garantizar la integridad, disponibilidad y seguridad de la información crítica de la entidad, realizar pruebas de intrusión intrusivas de caja gris o caja negra directamente en los entornos productivos activos y en horario hábil podría ocasionar caídas accidentales de servicio, bloqueo de bases de datos o corrupción de datos reales de los usuarios mineros.

Se solicita a la entidad confirmar que para la ejecución del Ethical Hacking sobre los 10 portales web, la ANM suministrará entornos de preproducción (staging o de pruebas) idénticos al entorno productivo y con bases de datos anonimizadas, de tal manera que las pruebas se realicen de forma segura sin afectar la disponibilidad del servicio al ciudadano.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

Las pruebas de penetración y Ethical Hacking sobre los diez (10) portales públicos se coordinarán previamente con el equipo de TI de la ANM y la supervisión del contrato. Según el tipo de portal y la criticidad del servicio, la Entidad dispondrá de entornos de pruebas/preproducción o autorizará ventanas de mantenimiento controladas para las evaluaciones en producción, garantizando la continuidad e integridad de la operación institucional.

Observación No. 35.

Información pública



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Documento: Anexo Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 7.5.

Tema: Consentimiento Habeas Data en pruebas de simulación de Phishing (Ingeniería Social).

Observación y solicitud: El contrato exige simular ataques de phishing sobre la totalidad de correos electrónicos de la ANM. Dado que estas pruebas implican el tratamiento y la simulación de engaños utilizando bases de datos que contienen correos corporativos y personales de funcionarios y contratistas de la entidad, se podría incurrir en violaciones a las directrices de la Ley 1581 de 2012 (Habeas Data) si los destinatarios no cuentan con un consentimiento informado previo sobre la realización de auditorías éticas de phishing por parte de la entidad.

Se solicita por ello a la entidad confirmar si cuenta con las autorizaciones vigentes de tratamiento de datos personales de su personal para realizar estos ejercicios éticos de intrusión simulada, liberando al contratista de toda responsabilidad civil, penal o legal que pueda derivarse del tratamiento de dicha información durante la prueba de ingeniería social.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La Agencia Nacional de Minería, en su calidad de responsable del tratamiento de datos y en el marco de sus políticas de seguridad de la información (MSPI), cuenta con el marco normativo institucional y las autorizaciones para la realización de auditorías éticas de ciberseguridad sobre sus plataformas y cuentas institucionales. El contratista ejecutará la prueba en estricto cumplimiento del objeto contractual y bajo la directriz del Oficial de Seguridad de la Entidad.

Observación No. 36.

Documento: Anexo Especificaciones y Requerimientos Técnicos Mínimos.

Página / Numeral: Literal 7.6 (Vicarius).

Tema: Responsabilidad en la instalación y despliegue del agente de software de Vicarius VRX.

Observación y solicitud: El Literal 7.6 estipula que el contratista debe suministrar e implementar la solución de gestión de vulnerabilidades Vicarius VRX para ciento cincuenta (150) licencias de endpoints de la ANM. Sin embargo, realizar la instalación manual máquina por máquina en los computadores de la entidad por parte del personal del proponente puede demorar meses y retrasar el cumplimiento de la puesta en servicio. El contratista debe proveer la consola y el instalador, pero la OTI cuenta con herramientas centralizadas (Microsoft Intune) de despliegue silencioso de agentes.

Se solicita aclarar que el contratista cumplirá con el ítem entregando la consola administrativa de Vicarius VRX configurada en la nube y suministrando el paquete instalador (agent), siendo responsabilidad de la OTI de la ANM ejecutar el despliegue y distribución automatizada del agente en las 150 estaciones de trabajo de sus funcionarios.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

Se confirma que el alcance del contratista para la solución Vicarius VRX comprende el suministro de la suscripción, la entrega de la consola administrativa en la nube debidamente configurada y la entrega del paquete de instalación (agent). El despliegue masivo y la distribución silenciosa en los 150 equipos de cómputo de la ANM se realizará a través de pruebas coordinadas entre el oferente y el equipo técnico de la ANM.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

El uso de herramientas automatizadas se realiza en la medida de la posibilidad, no obstante, el oferente deberá calcular su implementación a en acompañamiento al equipo técnico de ANM. Actualmente el cliente de Vicarius esta desplegado en los 150 servidores.

OBSERVACIONES PRESENTADAS POR TIVIT COLOMBIA

Observación No. 1

El Anexo Técnico exige transferir a la ANM los derechos patrimoniales de todo el material generado. Sin embargo, la Sección 13 del Pliego estipula que los productos no serán objeto de transferencia de los derechos patrimoniales a la ANM. Solicitamos aclarar qué régimen jurídico de propiedad intelectual aplicará definitivamente para el contrato.

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

La Agencia Nacional de Minería aclara y unifica el régimen de propiedad intelectual de la siguiente manera:

- **Licenciamiento y Software de Fabricantes / Terceros (Fortinet, Vicarius, Microsoft, etc.):** No se transfieren los derechos patrimoniales de las herramientas de software propietarias. El contratista concede u otorga a favor de la ANM las **licencias de uso, suscripciones y derechos de soporte directo** por la vigencia contratada (12 meses).
- **Entregables, Documentación y Desarrollos a Medida:** La propiedad intelectual y los derechos patrimoniales sobre los *informes, diagnósticos, guías, manuales de procedimiento, reglas de correlación personalizadas, playbooks y tableros (dashboards)* desarrollados específicamente para la ANM durante la ejecución contractual pertenecerán de forma exclusiva a la Agencia Nacional de Minería.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observación No. 2

Las suscripciones de los equipos FortiGate y FortiWeb vencieron el 30 de junio de 2026. El pliego prohíbe expresamente el cobro retroactivo de renovaciones, pero el fabricante Fortinet aplica obligatoriamente este recargo (back-billing). Solicitamos confirmar si la ANM asumirá directamente los costos de retroactividad facturados por el fabricante.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La Entidad reconoce las condiciones comerciales del fabricante Fortinet respecto a los cobros por reactivación/retroactividad (*back-billing*) cuando existe una interrupción en el periodo de soporte. No obstante, la ANM teniendo en cuenta los tiempos de adjudicación del presente contrato, a través del otrosí No. 2 al contrato SGR-055-2025 renovó las licencias correspondientes hasta el 30 de octubre de 2026.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

En ese sentido, se Aclara que el oferente deberá renovar por doce (12) meses el licenciamiento según el pliego de condiciones. Estas fechas serán actualizadas en el anexo técnico definitivo.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observación No. 3

Para la implementación del FortiSIEM en máquina virtual (VM), solicitamos confirmar: (i) si la ANM proveerá los recursos de procesamiento, RAM y licencias del hipervisor; y (ii) el almacenamiento físico disponible (en Terabytes) para garantizar la retención histórica de logs exigida (3 meses en línea y 12 meses fuera de línea)

RESPUESTA DE LA ENTIDAD: SE ACLARA.

- **(i) Recursos Virtualizados:** La ANM **suministrará la totalidad de los recursos de infraestructura virtual** (hipervisor VMware vSphere, cómputo vCPU, memoria RAM y direccionamiento IP).
- **(ii) Almacenamiento:** La ANM asignará y dispondrá en su almacenamiento SAN/Nube Institucional el espacio necesario para dar cumplimiento a los periodos de retención exigidos (3 meses para logs en línea de consulta rápida y 12 meses en repositorio frío/fuera de línea). El contratista debe dimensionar el consumo proyectado para que la OTI de la ANM efectúe la asignación del volumen de disco correspondiente.

Observación No. 4

El Cuadro de Cantidades incluye un Antivirus Alternativo para 300 Servidores. Solicitamos aclarar si el oferente debe suministrar e incluir el costo de estas licencias de software, o si la entidad ya dispone de ellas y el alcance del contratista se limita únicamente a la configuración, monitoreo e integración de logs en el SOC.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

Se INFORMA que la adquisición del licenciamiento para la solución de antivirus/endpoint para los servidores no hace parte del presente proceso de contratación. En ese sentido, se ACLARA que el alcance del contratista se limita de forma exclusiva a la **configuración, integración de conectores/logs en el SIEM/SOC, monitoreo, análisis de alertas y atención de incidentes** generados por dicha plataforma, sin requerir el suministro de licencias adicionales de software de antivirus por parte del oferente.

Observación No. 5

Se solicita realizar pruebas de penetración (Ethical Hacking) para diez (10) portales públicos de la ANM. Dado que el anexo técnico lista más de 19 portales web con infraestructuras y niveles de complejidad completamente diferentes, solicitamos definir taxativamente las URLs de los 10 portales seleccionados para dimensionar adecuadamente el esfuerzo de ingeniería.

RESPUESTA DE LA ENTIDAD: SE ACLARA.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

La Agencia Nacional de Minería aclara que las pruebas de penetración / Ethical Hacking se mantendrán acotadas al alcance cuantitativo de **diez (10) portales web públicos**. Las URLs específicas y definitivas que conformarán dicho alcance serán **definidas y notificadas formalmente por la ANM en la fase inicial de ejecución contractual**, previo al inicio de las pruebas y de común acuerdo con el supervisor del contrato y el contratista adjudicatario.

Para efectos de la estructuración de la propuesta técnica y económica, los oferentes deben considerar que el esfuerzo técnico de ingeniería comprende la evaluación de **10 aplicaciones/portales web públicos estándar de la Entidad**. Mantener la reserva o definición posterior de las URLs exactas permite a la ANM priorizar los activos con mayor nivel de exposición o cambios de infraestructura vigentes al momento del inicio de la ejecución, garantizando la pertinencia de las pruebas de seguridad sin alterar la carga de trabajo contratada

Observación No. 6.

El perfil del Analista de Ciberseguridad exige una (1) persona x 40 horas durante el periodo (12 meses de contrato) para brindar soporte en remediación de vulnerabilidades y coordinar pruebas de ingeniería social. Solicitamos aclarar si las 40 horas exigidas se refieren a una dedicación total anual, mensual o semanal, dado que 40 horas anuales resultan inviables para el alcance exigido.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La Entidad aclara que la dedicación requerida para el Analista de Ciberseguridad corresponde a una **bolsa mensual de hasta 40 horas laborables al mes**, las cuales serán distribuidas y requeridas bajo demanda conforme a las necesidades operativas de la ANM (soporte en remediación de vulnerabilidades, coordinación de campañas de ingeniería social, evaluaciones puntuales, etc.).

Observación No. 7.

El Acuerdo de Niveles de Servicio establece un tiempo de solución de una (1) hora para incidentes de prioridad alta. Debido a que gran parte de la infraestructura de la ANM es administrada o alojada por terceros (como el Data Center externo y redes MPLS), solicitamos incorporar una cláusula que excluya de la medición del SLA los retrasos imputables exclusivamente a dichos terceros

RESPUESTA DE LA ENTIDAD: SE ACLARA.

Se ACLARA que el contratista **no será sujeto a deducciones, multas o penalizaciones en la evaluación de los Acuerdos de Niveles de Servicio (ANS)** cuando los retrasos o indisponibilidades sean causados de manera comprobable por la falta de respuesta, caídas de servicio o demoras atinentes a proveedores terceros de la ANM (como el operador de canal de datos MPLS o el administrador del Data Center externo). El contratista deberá presentar la trazabilidad técnica de los *tickets* y escalamientos que evidencien dicha situación.

Observación No. 8

8. *Anexo Técnico (numeral 22) exige que la solución esté completamente operativa en un plazo máximo de 30 días calendario. Dado que la propia entidad estima una transición de aproximadamente dos (2) meses para la migración al nuevo SIEM, y con el fin de garantizar que los trabajos no afecten los servicios en horario*



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

hábil, solicitamos ampliar el plazo de implementación a sesenta (60) días calendario o autorizar un cronograma de entregas por fases.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La Entidad aclara la armonización de las fases del proyecto:

- **Fase 1 (Inicio Inmediato - Meses 1 y 2):** Operación en modalidad **SaaS transitorio** con el SOC del contratista para garantizar la continuidad del monitoreo desde el día 1 de ejecución.
- **Fase 2 (Inicio Inmediato / Meses 1 y 2 Implementación):** Despliegue en VM, *tuning*, migración de reglas y puesta en producción del **FortiSIEM propio de la ANM**.

Por lo tanto, el cronograma se ejecuta de manera coordinada por fases durante los 60 días del periodo de transición SaaS, sin interrumpir la operación de la Agencia.

Observación No. 9

9. *El Anexo Técnico exige la configuración e implementación de colectores de logs (incluyendo tres personalizados). Bajo la "Nota General" de abasto completo, solicitamos aclarar si la ANM proveerá la infraestructura virtual (máquinas virtuales en su plataforma VMware) para alojar estos colectores, o si el oferente debe suministrar el hardware físico o licencias para los servidores de recolección bajo su propio costo.*

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

La Agencia Nacional de Minería **suministrará los recursos de la plataforma de virtualización (VMware)** requeridos para alojar e instalar las instancias de los colectores de logs de FortiSIEM (incluyendo las VM necesarias para colectores personalizados). El contratista no deberá incluir hardware físico en su propuesta.

Observaciones No. 10 y 11:

10. *El pliego estipula que el servicio iniciará sobre el SIEM SaaS del proveedor y luego se migrará al FortiSIEM propio de la ANM. Solicitamos aclarar si durante la fase de transición (estimada en 2 meses) se requiere la operación simultánea y el doble monitoreo activo en ambas plataformas a la vez, o si la plataforma SaaS del proveedor se desactivará inmediatamente una vez el FortiSIEM de la entidad entre en producción.*

11. *La Nota 1 del numeral 2.3 del Pliego indica que el contratista debe transmitir y monitorear los eventos en un SIEM de propiedad del oferente durante todo el tiempo de ejecución. No obstante, el Ítem 8 y el literal 7.2 exigen la adquisición, implementación y migración del servicio al FortiSIEM propio de la ANM. Solicitamos aclarar si el contratista debe operar su SIEM propio en paralelo con el FortiSIEM de la entidad durante todo el contrato, o si la plataforma del oferente solo se usará durante los dos (2) meses de transición.*

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La plataforma SIEM SaaS del contratista **se utilizará única y exclusivamente durante los dos (2) primeros meses del contrato (fase de transición y empalme)**. Una vez finalizada la implementación y aprobación de la puesta en marcha del FortiSIEM en la máquina virtual de la ANM, el monitoreo continuará de forma definitiva



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

sobre el FortiSIEM de la Entidad y la plataforma SaaS del proveedor se desactivará, evitando la duplicidad permanente de cargas de trabajo.

Observación No. 12

12. *El pliego exige certificación Tier III de Uptime Institute o ICREA Nivel IV para la sede física del SOC. No obstante, dado que se permite que la plataforma de monitoreo sea CLOUD, la oficina física donde operan los analistas actúa únicamente como canal de visualización y gestión mediante conexiones cifradas y MFA.*

Bajo el estándar ISO/IEC 27001:2022 (Controles 7.1 y 7.3), la seguridad de estas áreas operativas se garantiza mediante controles de acceso físico y lógico, mas no con la redundancia electromecánica (energía y climatización) propia de un Data Center (Tier III). Exigir este requisito para la sede de analistas es desproporcionado y limita la libre concurrencia (Art. 5 Ley 1150 de 2007). Solicitamos limitar la certificación Tier III de forma exclusiva al Data Center donde se aloje la plataforma Cloud y permitir para la sede física del oferente la acreditación de controles bajo ISO 27001.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

En alineación con la respuesta dada a otras observaciones sobre la materia, la ANM aclara que **la certificación TIER III (Uptime Institute) o ICREA Nivel IV se exige de forma exclusiva para el Data Center (Principal/Secundario)** que aloja los servidores y el core de la infraestructura del SOC/SIEM.

Observaciones No. 13 y 14

13. *El pliego establece que el servicio iniciará sobre la solución SIEM SaaS actual para luego migrar al nuevo FortiSIEM de la ANM. Solicitamos aclarar: (i) ¿El alcance de la migración comprende únicamente elementos de configuración (reglas de correlación, alertas, conectores y tableros) o incluye también la transferencia de la data histórica de logs acumulada en el SIEM SaaS actual? (ii) En caso de requerirse la migración del historial de logs, ¿esta información debe cargarse en el SIEM del oferente durante el periodo de transición o directamente en el FortiSIEM definitivo de la entidad?*

14. *¿Cuál es la marca o tecnología del SIEM SaaS que opera actualmente la entidad? (ii) ¿Cuál es la cantidad exacta de reglas de correlación, alertas personalizadas, conectores específicos, tableros de control (dashboards) y casos de uso activos que se encuentran configurados actualmente y que el contratista deberá migrar, replicar o afinar en el nuevo FortiSIEM?*

RESPUESTA DE LA ENTIDAD: SE ACLARA.

- **(i) Data Histórica:** La migración NO contempla la transferencia de logs de la plataforma actual al nuevo FORTISIEM ANM .
- **(ii) Tecnología Actual y Métricas de Migración:** Actualmente el proveedor externo tiene tecnología FORTISIEM lo cual facilitará la migración de reglas de correlación al nuevo FORTISIEM ANM. Con base en este contrato tenemos correlaciónamiento de 5 fuentes establecidas en el ANEXO TECNICO y 10 reglas de correlación, 2 colectores y 1 supervisor de marca FORTINET.
- **(iii) NOTA.** El contratista apoyará la exportación de la regla de correlación, sin limitarse a ellas. Se Clara que la ANM estima correlacionar fuentes adicionales a las actualmente contratadas, en cuyo caso será de obligación del proveedor realizar las respectivas reglas y

RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

configuraciones hasta un máximo de 50 fuentes de correlación. Los cuáles serán acordados entre el proveedor y el supervisor del contrato.

OBSERVACIONES PRESENTADAS POR OLIMPIA IT SAS

Observación No. 1

No.	Documento	Numeral	Pagina	Texto Observado	Observación/Solicitud
1	Anexo especificaciones y requerimientos técnicos mínimos	5	8	3. Todo el material (documentos, audios, tablas, videos, etc.) generado durante la ejecución debe ser entregado a la ANM, señalando claramente los nombres de los autores y la transferencia de los derechos patrimoniales sobre los mismos a la ANM, sin que el contratista conserve copia de ellos.	Se solicita amablemente modificar la disposición según la cual el contratista no podrá conservar copia del material generado durante la ejecución del contrato, con el fin de permitir la conservación de una copia de los entregables y demás soportes documentales durante la vigencia del contrato y el término que resulte necesario para acreditar el cumplimiento de las obligaciones contractuales, atender procesos de seguimiento, auditoría, informes o requerimientos

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La ANM aclara que el contratista **podrá conservar una copia de respaldo estrictamente para efectos de archivo documental, auditoría interna y soporte de cumplimiento contractual**. No obstante, sobre dicha información recae el deber legal y contractual de estricta confidencialidad, reserva y protección de datos personales de conformidad con la Ley 1581 de 2012, no pudiendo el contratista comercializar, ceder ni difundir dicho material bajo ninguna circunstancia. (En línea con lo dispuesto en la Respuesta a la Observación No. 1 de TIVIT Colombia).

Observaciones No. 2 y No. 3:

No.	Documento	Numeral	Pagina	Texto Observado	Observación/Solicitud
-----	-----------	---------	--------	-----------------	-----------------------



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

2	Anexo especificaciones y requerimientos técnicos mínimos	9	44	El proveedor, en los cuales que aplique, debe otorgar extensión de garantía directamente con el fabricante, para todos y cada una de las licencias	Se solicita aclarar el alcance del requisito, indicando expresamente qué debe entenderse por "extensión de garantía" respecto de las licencias de software, así como los productos a los que aplica dicha obligación.
3	Anexo especificaciones y requerimientos técnicos mínimos	9	44	El proveedor, en los cuales que aplique, debe otorgar extensión de garantía directamente con el fabricante, para todos y cada una de las licencias.	Se solicita aclarar el alcance del requisito, precisando a qué se refiere la expresión "en los cuales que aplique", indicando expresamente cuáles licencias o productos deberán contar con extensión de garantía directamente con el fabricante y bajo qué criterios se determinará su aplicación.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La extensión de garantía corresponde a la suscripción y soporte técnico directo otorgado por las casas matrices de los fabricantes (Fortinet, Vicarius, etc.) por un periodo de doce (12) meses. Dicha condición aplica para los **Ítems 6, 7, 8 y 9** (Renovación Fortinet, Vicarius VRX, FortiSIEM VM y FortiPAM), e incluye el acceso a actualizaciones de software, parches de seguridad, bases de datos de firmas de amenazas, soporte técnico de nivel 3 directo con el fabricante y reemplazo de licenciamiento.

Observaciones No. 4 y No. 5:

N o.	Documento	Numeral	Página	Texto Observado	Observación/Solicitud
------	-----------	---------	--------	-----------------	-----------------------

RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

4	Anexo especificaciones y requerimientos técnicos mínimos	11	45	Los servicios ofrecidos en el presente contrato deberán tener una disponibilidad del 99,60% y las compensaciones por su no cumplimiento se aplicarán de acuerdo con la siguiente tabla: <table><tr><th colspan="2">RANGO % DISPONIBILIDAD</th><th>INDISPONIBILIDAD EN HORAS CALENDARIO</th><th>COMPENSACIÓN TA</th></tr><tr><td>100</td><td>99.60</td><td>2.88</td><td></td></tr><tr><td>99.59</td><td>98</td><td>14.4</td><td></td></tr><tr><td>97.99</td><td>96</td><td>28.8</td><td></td></tr><tr><td>95.99</td><td>90</td><td>72</td><td></td></tr><tr><td>89.99</td><td>Menor que 89.99</td><td>Más de 72 Horas de Indisponibilidad al mes</td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>	RANGO % DISPONIBILIDAD		INDISPONIBILIDAD EN HORAS CALENDARIO	COMPENSACIÓN TA	100	99.60	2.88		99.59	98	14.4		97.99	96	28.8		95.99	90	72		89.99	Menor que 89.99	Más de 72 Horas de Indisponibilidad al mes						Se solicita respetuosamente revisar el esquema de compensaciones previsto para los Acuerdos de Nivel de Servicio (ANS), con el fin de que las mismas guarden un criterio de proporcionalidad respecto del incumplimiento presentado. En ese sentido, se propone que las compensaciones se calculen únicamente sobre el valor mensual del servicio, componente o funcionalidad efectivamente afectada por la indisponibilidad, y no sobre la totalidad de la facturación mensual del contrato, toda vez que este comprende múltiples servicios y
RANGO % DISPONIBILIDAD		INDISPONIBILIDAD EN HORAS CALENDARIO	COMPENSACIÓN TA																														
100	99.60	2.88																															
99.59	98	14.4																															
97.99	96	28.8																															
95.99	90	72																															
89.99	Menor que 89.99	Más de 72 Horas de Indisponibilidad al mes																															



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

					componentes independientes cuya prestación puede mantenerse de manera normal aun cuando se presente una afectación puntual en alguno de ellos. De igual manera, agradecemos puedan confirmar a que servicios les aplicaría este ANS																																								
5	Anexo especificaciones y requerimientos técnicos mínimos	11	45	Los servicios ofrecidos en el presente contrato deberán tener una disponibilidad del 99,6% mensual y las compensaciones por su no cumplimiento se aplicarán de acuerdo con la siguiente tabla: <table><tr><th colspan="2">RANGO</th><th colspan="2">INDISPONIBILIDAD</th><th>COMPENSACION SOBRE</th></tr><tr><th colspan="2">% DISPONIBILIDAD</th><th colspan="2">EN HORAS CALENDARIO</th><th>TARIFA MENSUAL</th></tr><tr><td>100</td><td>99.60</td><td colspan="2">2.88</td><td>0%</td></tr><tr><td>99.59</td><td>98</td><td colspan="2">14.4</td><td>5%</td></tr><tr><td>97.99</td><td>96</td><td colspan="2">28.8</td><td>20%</td></tr><tr><td>95.99</td><td>90</td><td colspan="2">72</td><td>50%</td></tr><tr><td>89.99</td><td>Menor que 89.99</td><td colspan="2">Más de 72 Horas de</td><td>100%</td></tr><tr><td></td><td></td><td colspan="2">Indisponibilidad al mes</td><td></td></tr></table>	RANGO		INDISPONIBILIDAD		COMPENSACION SOBRE	% DISPONIBILIDAD		EN HORAS CALENDARIO		TARIFA MENSUAL	100	99.60	2.88		0%	99.59	98	14.4		5%	97.99	96	28.8		20%	95.99	90	72		50%	89.99	Menor que 89.99	Más de 72 Horas de		100%			Indisponibilidad al mes			Se solicita amablemente revisar los porcentajes de compensación establecidos por incumplimiento de los Acuerdos de Nivel de Servicio (ANS), proponiendo que estos se establezcan en un rango gradual entre el 1% y el 5% del valor mensual del servicio o componente afectado, en atención a
RANGO		INDISPONIBILIDAD		COMPENSACION SOBRE																																									
% DISPONIBILIDAD		EN HORAS CALENDARIO		TARIFA MENSUAL																																									
100	99.60	2.88		0%																																									
99.59	98	14.4		5%																																									
97.99	96	28.8		20%																																									
95.99	90	72		50%																																									
89.99	Menor que 89.99	Más de 72 Horas de		100%																																									
		Indisponibilidad al mes																																											



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

				criterios de razonabilidad y proporcionalidad . Lo anterior, considerando que las compensaciones tienen una finalidad de incentivar el cumplimiento de los ANS. En este sentido, porcentajes de compensación de hasta el 20%, 50% o incluso el 100% de la tarifa mensual resultan desproporcionados frente a desviaciones parciales en los niveles de disponibilidad, pudiendo generar un desequilibrio económico del contrato y trasladar al contratista riesgos que exceden el alcance del servicio prestado. En
--	--	--	--	---



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

					consecuencia, se propone establecer un esquema de compensaciones escalonado, con porcentajes entre el 1% y el 5%, suficiente para incentivar el cumplimiento de los ANS, preservando al mismo tiempo los principios de proporcionalidad .
--	--	--	--	--	---

RESPUESTA DE LA ENTIDAD: NO SE ACOGEN LAS SOLICITUDES.

La operación del Centro de Operaciones de Seguridad (SOC) y el monitoreo de ciberseguridad constituyen un servicio integral donde la indisponibilidad de un componente afecta directamente la postura de ciberdefensa de la ANM. La tabla de disponibilidad (\$99,60\% mínimo mensual) y el escalonamiento de compensaciones publicados en el numeral 11 del Anexo Técnico guardan estricta proporcionalidad con el riesgo institucional. Las deducciones se aplican sobre la tarifa mensual del servicio administrado correspondiente.

Observación No. 6:

No.	Documento	Numeral	Pagina	Texto Observado	Observación/Solicitud
6	Proyecto pliego de condiciones	2.4	15	La vigencia del contrato será de doce (12) meses, contados a partir de la suscripción del acta de inicio, previo al cumplimiento de los requisitos de perfeccionamiento y ejecución	Entendemos que el plazo de doce (12) meses corresponde al periodo de operación del servicio. No obstante, agradeceríamos confirmar si los componentes que requieren una etapa de implementación cuentan con un periodo previo e independiente para su ejecución, o si, por el contrario, dicha implementación se encuentra comprendida dentro

RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

					de los doce (12) meses de ejecución contractual.
--	--	--	--	--	--

RESPUESTA DE LA ENTIDAD: SE ACLARA.

El plazo de ejecución del contrato es de **doce (12) meses contados a partir de la firma del acta de inicio**. Las actividades de implementación y migración (servicio SaaS de transición durante los dos primeros meses y despliegue del FortiSIEM/FortiPAM) se ejecutan de manera concomitante dentro de dicho plazo contractual de 12 meses, garantizando la continuidad del monitoreo.

(Remitirse a la Respuesta No. 8 de *TIVIT Colombia* y No. 21 de *Grupo Licitaciones G*).

Observación No. 7: Dinámica de la Subasta Inversa Electrónica

No.	Documento	Numeral	Página	Texto Observado	Observación/Solicitud
7	Proyecto pliego de condiciones	3.8	43	La subasta culminará una vez se cumple el tiempo establecido para la realización de la misma y no se realicen más lances válidos.	¿Esto significa que, aun cuando la subasta se encuentre en sus últimos minutos, la presentación de un nuevo lance daría lugar a la extensión del tiempo establecido para su finalización? De ser así, ¿Cuánto tiempo de extensión sería?

RESPUESTA DE LA ENTIDAD: SE ACLARA.

De acuerdo con las reglas de operación de la plataforma SECOP II de la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente (CCE), si se presenta un lance válido durante los últimos minutos del periodo de subasta, el sistema activa de forma automática un periodo de extensión (lance de desempate/extensión) de tres **(3) minutos adicionales**, garantizando el principio de libre competencia y selección objetiva.

Observación No. 8:

No.	Documento	Numeral	Página	Texto Observado	Observación/Solicitud
-----	-----------	---------	--------	-----------------	-----------------------



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

8	Borrador clausulado complementario del contrato	Décima	10	MULTAS: En caso de mora o incumplimiento parcial de las obligaciones adquiridas por EL CONTRATISTA, LA AGENCIA podrá cobrar multas diarias y sucesivas equivalentes al cero punto cinco por ciento (0.5%) del valor total de este contrato, por cada día de retardo o incumplimiento, sin que el monto total de la multa exceda el veinte por ciento (20%) de su valor total.	Solicitamos respetuosamente que el límite máximo de las multas sea ajustado al cinco por ciento (5%) del valor total del contrato, en lugar del veinte por ciento (20%) previsto en la cláusula. Lo anterior, considerando que las multas tienen como finalidad apremiar el cumplimiento oportuno de las obligaciones contractuales. En ese sentido, un tope del veinte por ciento (20%) resulta excesivo frente a la naturaleza de este mecanismo. Adicionalmente, un límite máximo del cinco por ciento (5%) constituye un porcentaje ampliamente utilizado en la contratación pública y privada para este tipo de mecanismos, permitiendo a la Entidad contar con una herramienta eficaz para incentivar el cumplimiento de las obligaciones, sin desnaturalizar la finalidad de las multas ni afectar la proporcionalidad que debe regir este tipo de estipulaciones.
---	--	--------	----	--	--

RESPUESTA DE LA ENTIDAD: NO SE ACOGE LA SOLICITUD.

El tope máximo acumulado de multas del **veinte por ciento (20%)** del valor del contrato corresponde al límite legal fijado en la normatividad de contratación estatal (artículo 86 de la Ley 1474 de 2011). Dicho porcentaje

RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

busca conminar al contratista al cumplimiento oportuno en un contrato que protege la infraestructura tecnológica crítica del Estado.

Observación No. 9:

No.	Documento	Numeral	Pagina	Texto Observado	Observación/Solicitud
9	Anexo Técnico	Operación SOC	N/A	Prestación del servicio SOC 7x24x365.	Agradecemos a la entidad publicar el inventario detallado de los activos que harán parte del monitoreo, indicando cantidades de servidores, equipos de seguridad, dispositivos de red, aplicaciones críticas y servicios en nube, con el fin de dimensionar adecuadamente el servicio requerido.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

Sugerimos remitirse a la **Respuesta No. 2 brindada a SecureSoft Colombia** y a la **Respuesta No. 2 de WEXLER S.A.S.**. La ANM ha puesto a disposición el panorama general de su infraestructura (servidores físicos/virtuales, switches, etc.) y reitera que las fuentes a ingresar directamente al SIEM corresponden a las 50 fuentes estratégicas licenciadas (1000 EPS).

Observaciones No. 10 y No. 28:

No.	Documento	Numeral	Pagina	Texto Observado	Observación/Solicitud
10	Anexo Técnico	Administración de plataformas	N/A	Administración de plataformas Fortinet y Microsoft.	Agradecemos a la entidad publicar el inventario de las plataformas objeto de administración, indicando modelo, versión de software, cantidad de equipos y estado del soporte vigente.
28	Anexo Técnico	Crecimiento de infraestructura	N/A	Incorporación de nuevos activos durante la ejecución.	Agradecemos a la entidad aclarar el procedimiento que se aplicará en caso de incrementarse el número de activos, dispositivos o servicios durante la vigencia

RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

					del contrato, indicando si dicho crecimiento hace parte del alcance contratado o dará lugar a un ajuste contractual.
--	--	--	--	--	--

RESPUESTA DE LA ENTIDAD: SE ACLARA.

Remitirse a la **Respuesta No. 28 dada a Grupo Licitaciones G**. Los números de serie y modelos exactos de la plataforma Fortinet serán incluidos en el Anexo de Especificaciones y Requerimiento Técnicos que se publicarán en los documentos definitivos del presente proceso de contratación. Respecto al crecimiento, la integración de nuevos activos dentro de las capacidades máximas contratadas (hasta 50 dispositivos / 1000 EPS) no generará costos adicionales; si la infraestructura supera el límite licenciado, situación que será informada en su oportunidad por parte de la supervisión dentro de la ejecución contractual.

Observación No. 11:

No.	Documento	Numeral	Página	Texto Observado	Observación/Solicitud
11	Anexo Técnico	Microsoft Sentinel	N/A	Administración y monitoreo de Sentinel.	Agradecemos a la entidad confirmar si Microsoft Sentinel ya se encuentra implementado y operando en producción o si el contratista deberá realizar actividades adicionales de configuración o puesta en marcha.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

Se sugiere remitirse a la **Respuesta No. 29 brindada a Grupo Licitaciones G**. pero se aclara que Microsoft Sentinel actualmente NO se encuentra implementado en la ANM. Pero una vez sea implementado por la ANM El alcance del contratista comprende la administración lógica, *tuning*, configuración de reglas y monitoreo de alertas hacia el SOC, asumiendo la ANM los costos de licenciamiento e ingesta en Azure.

Observación No. 12:

No.	Documento	Numeral	Página	Texto Observado	Observación/Solicitud
12	Anexo Técnico	Servicio SIEM	N/A	SIEM SaaS durante la implementación de FortiSIEM.	Agradecemos a la entidad indicar el volumen estimado de eventos por segundo (EPS) y el promedio diario de generación de logs, con el fin de dimensionar



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

					adecuadamente el servicio temporal de SIEM SaaS.
--	--	--	--	--	--

RESPUESTA DE LA ENTIDAD: SE ACLARA.

Remitirse a la **Respuesta No. 21** brindada a **Grupo Licitaciones G** y **No. 1 de WEXLER S.A.S.**. La capacidad para la etapa transitoria SaaS (meses 1 y 2) es de 512 EPS filtrados diarios.

Observaciones No. 13, 14 y 15:

No.	Documento	Numeral	Pagina	Texto Observado	Observación/Solicitud
13	Anexo Técnico	Integración SIEM	N/A	Integración de múltiples fuentes.	Agradecemos a la entidad publicar el listado de las fuentes de información que deberán integrarse al SIEM, indicando el tipo de dispositivo o aplicación y el volumen estimado de eventos por cada una.
14	Anexo Técnico	FortiSIEM	N/A	Implementación de FortiSIEM.	Agradecemos a la entidad indicar si la infraestructura de virtualización requerida para FortiSIEM será suministrada por la Entidad o si hace parte del alcance del contratista.
15	Anexo Técnico	FortiPAM	N/A	Implementación de FortiPAM.	Agradecemos a la entidad indicar si la Entidad dispone actualmente de infraestructura y componentes necesarios para la implementación de FortiPAM o si éstos deberán ser considerados dentro del proyecto.

RESPUESTA DE LA ENTIDAD:

Remitirse a las **Respuestas No. 3 y No. 9 de TIVIT Colombia** y a las **Respuestas FortiSIEM No. 3 y FortiPAM No. 2 de WEXLER S.A.S.**. La ANM suministrará el 100% de la infraestructura virtual (hipervisor VMware, vCPU, RAM, almacenamiento y red) para el despliegue de FortiSIEM, FortiPAM y colectores.

Observaciones No. 16, 17 y 18:



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

No.	Documento	Numeral	Página	Texto Observado	Observación/Solicitud
16	Anexo Técnico	Vulnerability Assessment	N/A	Ejecución de análisis de vulnerabilidades.	Agradecemos a la entidad publicar el alcance del análisis de vulnerabilidades indicando la distribución de activos entre infraestructura interna, infraestructura externa, aplicaciones web y ambientes en nube, si aplica.
17	Anexo Técnico	Pentesting	N/A	Pruebas de Ethical Hacking.	Agradecemos a la entidad publicar el listado de aplicaciones o portales objeto de las pruebas de Pentesting, indicando si corresponden a aplicaciones internas, externas o publicadas en Internet.
18	Anexo Técnico	Ingeniería Social	N/A	Campañas de Ingeniería Social.	Agradecemos a la entidad indicar el número aproximado de usuarios que participarán en las campañas de ingeniería social y los canales autorizados para su ejecución (correo electrónico, llamadas, SMS u otros).

RESPUESTA DE LA ENTIDAD:

Remitirse a las respuestas otorgadas a *Grupo Licitaciones G* (Respuestas No. 25, No. 31 y No. 35) y *TIVIT Colombia* (Respuesta No. 5):

1. **Análisis de Vulnerabilidades:** 100 direcciones IP estratégicas con Re-Test semestral sobre el mismo alcance.
2. **Pentesting:** 10 portales web públicos expuestos, cuyas URLs serán notificadas al inicio de la ejecución.
3. **Ingeniería Social:** Hasta 1.850 usuarios/buzones corporativos en campañas de phishing.

Observaciones No. 19 y 20:

No.	Documento	Numeral	Página	Texto Observado	Observación/Solicitud
19	Anexo Técnico	Renovación Vicarius	N/A	Renovación de 150 licencias.	Agradecemos a la entidad indicar el tipo de



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

					licenciamiento actualmente instalado (endpoint, servidor u otro), así como su fecha de vencimiento.
20	Anexo Técnico	VPN/ZTNA	N/A	Renovación de 700 licencias.	Agradecemos a la entidad confirmar si las licencias requeridas corresponden a usuarios nominales o concurrentes.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

1. **Vicarius VRX:** 150 licencias para endpoints. El contratista entrega consola e instalador, y la OTI de la ANM en conjunto con el proveedor realiza el despliegue necesario en los 150 servidores (Respuesta No. 36 de *Grupo Licitaciones G*).
2. **ZTNA / VPN:** 1.700 licencias de agentes para **usuarios nominales** vinculados a la Entidad.

Observación No. 21:

No.	Documento	Numeral	Pagina	Texto Observado	Observación/Solicitud
21	Anexo Técnico	ANS	N/A	Prestación del servicio.	Agradecemos a la entidad publicar la matriz completa de Acuerdos de Niveles de Servicio (ANS), incluyendo tiempos de respuesta, solución, escalamiento y criterios de medición de cumplimiento.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

La matriz de ANS se encuentra contenida en el numeral 11 del Anexo Técnico: Tiempos de respuesta para Prioridad Alta = 15 min / Solución = 1 hora; Prioridad Media = 1 hora / Solución = 2 horas; Prioridad Baja = 12 horas / Solución = 12 horas; con una disponibilidad mínima global del 99,60% mensual.

Observaciones No. 22, 23 y 29:

No.	Documento	Numeral	Pagina	Texto Observado	Observación/Solicitud
22	Proyecto de Pliego	Experiencia	N/A	Experiencia del proponente.	Agradecemos a la entidad permitir que la experiencia pueda acreditarse mediante contratos cuyo objeto contemple servicios



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

					administrados de ciberseguridad, operación SOC, administración de plataformas de seguridad o servicios equivalentes, sin exigir que todas las actividades se encuentren concentradas en un único contrato, promoviendo una mayor pluralidad de oferentes.
23	Proyecto de Pliego	Experiencia	N/A	Contratos similares.	Agradecemos a la entidad aclarar que la experiencia podrá acreditarse mediante contratos ejecutados tanto para entidades públicas como privadas, siempre que el objeto y alcance sean equivalentes al requerido.
29	Proyecto pliego de condiciones	6.2	62	El proponente que oferte para la presente contratación deberá acreditar experiencia máxima de cinco (05) contratos ejecutados y/o terminados y/o liquidados al cierre del presente proceso de contratación, cuyo objeto y obligaciones incluya la implementación de soluciones de seguridad informática en	Respetuosamente solicitamos a la Entidad ajustar el requisito de experiencia habilitante, de manera que no se limite exclusivamente a contratos de implementación de soluciones de seguridad informática, sino que también permita acreditar experiencia relacionada con la operación, administración, monitoreo y gestión de servicios de ciberseguridad y Centros de Operaciones de Seguridad (SOC). Lo anterior teniendo en cuenta que el objeto contractual incluye una participación altamente relevante de actividades de operación continua, tales como monitoreo 7x24x365, gestión de incidentes de seguridad,



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

			entidades públicas o privadas. En todo caso, la experiencia que pretenda acreditar el oferente debe atender los siguientes parámetros y condiciones: (i) Dos (2) de los contratos allegados deberán contener obligaciones o actividades que incluyan la implementación de soluciones de seguridad informática en entidades estatales o privadas.	correlación de eventos SIEM, administración de plataformas de seguridad, gestión de accesos privilegiados, generación de alertas y respuesta ante incidentes, actividades que constituyen servicios especializados de operación más que de simple implementación. En consecuencia, restringir la experiencia únicamente a contratos de implementación limita injustificadamente la pluralidad de oferentes, desconociendo que existen empresas con amplia trayectoria y especialización en la prestación de servicios SOC administrados, monitoreo de seguridad, MDR, SIEM, gestión de incidentes, operación de plataformas de ciberseguridad y administración de infraestructura de seguridad, experiencia que guarda relación directa con las obligaciones principales del futuro contrato. Por lo anterior, solicitamos que el requisito quede establecido en términos amplios, permitiendo acreditar contratos cuyo objeto incluya cualquiera de las siguientes actividades: Implementación de soluciones de seguridad informática. Operación de Centros de Operaciones de Seguridad (SOC).
--	--	--	--	--



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

					Monitoreo y gestión de eventos de seguridad. Administración y operación de plataformas SIEM. Gestión y atención de incidentes de ciberseguridad. Servicios administrados de seguridad (MSSP). Administración de herramientas de seguridad informática y protección perimetral. Propuesta de redacción “El proponente deberá acreditar experiencia mediante contratos ejecutados, terminados o liquidados cuyo objeto o alcance incluya la implementación, operación, administración, monitoreo o gestión de soluciones y servicios de seguridad informática, ciberseguridad o Centros de Operaciones de Seguridad (SOC), en entidades públicas o privadas.” Esta modificación mantiene la relación con el objeto contractual y favorece los principios de selección objetiva, libre concurrencia y pluralidad de oferentes, permitiendo la participación de empresas con experiencia efectiva y pertinente en la prestación de servicios especializados de ciberseguridad que constituyen el núcleo funcional del contrato.
--	--	--	--	--	--

RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

RESPUESTA DE LA ENTIDAD: SE ACOGE LA SOLICITUD Y SE ACLARA.

Remitirse a la **Respuesta No. 2 otorgada a Grupo Licitaciones G**. La ANM aceptará contratos cuyo objeto o alcance incluya *implementación, operación, administración, monitoreo o gestión de soluciones de ciberseguridad, servicios administrados MSSP o Centros de Operaciones de Seguridad (SOC)* en entidades públicas o privadas.

En consecuencia, los ajustes anteriormente señalados se verán reflejados en los documentos definitivos del presente proceso de contratación.

Observaciones No. 24, 25 y 26:

No.	Documento	Numeral	Página	Texto Observado	Observación/Solicitud
24	Anexo Técnico	Personal mínimo	N/A	Perfiles requeridos.	Agradecemos a la entidad permitir la homologación de experiencia profesional en proyectos de ciberseguridad y operación SOC para los perfiles mínimos exigidos, siempre que se acrediten las competencias requeridas para la ejecución del contrato.
25	Anexo Técnico	Certificaciones	N/A	Certificaciones del personal.	Agradecemos a la entidad aceptar certificaciones equivalentes emitidas por fabricantes o entidades reconocidas internacionalmente que acrediten competencias similares a las exigidas, favoreciendo la pluralidad de oferentes.
26	Anexo Técnico	Personal mínimo	N/A	Equipo de trabajo.	Agradecemos a la entidad aclarar si el personal mínimo requerido deberá tener dedicación exclusiva al contrato o si podrá atender otros proyectos, siempre que se garantice el cumplimiento de los ANS y las obligaciones contractuales.

RESPUESTA DE LA ENTIDAD: SE ACOGE PARCIALMENTE Y SE ACLARA.

Formación y Certificaciones: Remitirse a las Respuestas No. 5 a No. 18 de *Grupo Licitaciones G*. Se ampliaron los títulos del NBC SNIES y las certificaciones equivalentes para Coordinador y Analista (CompTIA, ISO, etc.). Se mantiene la certificación de Fortinet (NSE4+) para el Profesional Senior por administrar los equipos perimetrales de la ANM.



RESPUESTA OBSERVACIONES PROCESO SASI-007-2026

Dedicación: El Profesional Senior tiene dedicación de tiempo completo 5x8 (remoto desde el SOC con desplazamientos a la ANM si se requiere); el Analista tiene una bolsa mensual de 40 horas; y el Coordinador tiene dedicación parcial según necesidades. (Respuesta No. 22 de *Grupo Licitaciones G*).

Observación No. 27: Contenido de Informes Mensuales

No.	Documento	Numeral	Página	Texto Observado	Observación/Solicitud
27	Anexo Técnico	Informes	N/A	Informes mensuales.	Agradecemos a la entidad indicar el contenido mínimo esperado de los informes técnicos y ejecutivos, así como los criterios de aceptación por parte de la supervisión del contrato.

RESPUESTA DE LA ENTIDAD: SE ACLARA.

Los informes mensuales deben consolidar: (1) Resumen ejecutivo de incidentes atendidos por severidad; (2) Métricas de disponibilidad y cumplimiento de ANS; (3) Reporte de ingesta de eventos e indicadores del SIEM; (4) Estado de salud y cambios en plataformas perimetrales (Fortinet, PAM, Defender); y (5) Plan de recomendaciones de seguridad. (6) Gestión de eventos e incidentes. (7) cuando aplique, estado o reporte de la plataforma PAM (8) Estado de seguridad de Microsoft Defender o plataforma 365. La supervisión contará con 5 días hábiles para su revisión y aprobación.

COMITÉ ESTRUCTURADOR

LUIS ALONSO LUGO CHARRY
Contratista OTI

SONIA OCHOA SANABRIA
Componente jurídico OTI

PAOLO BONILLA RODRIGUEZ
Componente jurídico OTI