



Bogotá, 15-10-2026 15:54 PM

PARA: **ADRIANA MILENA LÓPEZ VASQUEZ**
Coordinadora Grupo de Contratación

DE: **ANDREA BIBIANA PEÑA GÓMEZ**
Jefe Oficina de Tecnología e Información (E)

ASUNTO: Solicitud de expedición de Adenda No. 1 – Proceso de Selección SA-SI-007-2026

Cordial saludo,

Conforme a las observaciones allegadas al proceso de la referencia SA-SI-007-2026, cuyo objeto corresponde a *“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” (Línea PAA 130005426_613000126)*”, y teniendo en cuenta que algunas de ellas fueron aceptadas por la entidad, lo cual conlleva en esta etapa del proceso necesariamente la modificación o ajuste de algunos apartes de la invitación pública, se requiere que se proceda a realizar la correspondiente adenda No. 1 conforme lo establece el Decreto 1082 de 2015 el cual en su artículo 2.2.1.1.2.2.1, determina que:

(...) 2.2.1.1.2.2.1 Modificación de los pliegos de condiciones. La Entidad Estatal puede modificar los pliegos de condiciones a través de Adendas expedidas antes del vencimiento del plazo para presentar ofertas (...)

En este orden de ideas se procede a determinar los numerales que serán objeto de modificación, así:

PRIMERO: MODIFIQUESE, el numeral 13.3.. del Estudio Previo conforme las descripciones y ajustes que se describen a continuación:

13.3. CERTIFICACIONES RELACIONADAS CON EL SOC (CENTRO DE OPERACIONES DE SEGURIDAD) DEL PROPONENTE

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

- *Certificación emitida por el representante legal del proponente en el que se*



haga constar que los servicios objeto de la presente contratación serán prestados en el SOC de propiedad del oferente.

- *Certificación TIER III del Uptime Institute o ICREA Nivel IV, donde se encuentra implementado el SOC*
- *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 y/o Especialidad Security Operations*
- *Contar y aportar reporte SOC 2 (Tipo II) vigente, y/o reporte SOC 3 vigente, y/o acreditación del marco de madurez SOMM (Security Operations Maturity Model) realizada por un tercero independiente.*

SEGUNDO: MODIFÍQUESE, el numeral 7.1.7. del Anexo de Especificaciones y Requerimientos Técnicos Mínimos conforme las descripciones y ajustes que se describen a continuación:

7.1.7.	<i>El SOC debe estar acreditado como MSSP (Managed Security Service Provider) por el fabricante FORTINET, correspondiente a la plataforma FortiSIEM requerida para la prestación del servicio y en alineación con la homogeneidad tecnológica de la Entidad. Adicionalmente, el proponente deberá contar con reporte SOC 2 (Tipo II) vigente, y/o reporte SOC 3 vigente, y/o acreditación del marco de madurez SOMM (Security Operations Maturity Model) realizada por un tercero independiente.</i>	
--------	--	--

TERCERO: MODIFÍQUESE, el numeral 7.1.23 del Anexo de Especificaciones y Requerimientos Técnicos Mínimos conforme las descripciones y ajustes que se describen a continuación:

7.1.23.	<i>Al inicio de la ejecución del contrato, el contratista deberá prestar el servicio de monitoreo SOC sobre la solución SIEM de su propiedad, la cual deberá ser operada bajo la modalidad de Software como Servicio (SaaS), garantizando la continuidad del monitoreo y la gestión de eventos de seguridad de la información de la ANM.</i> <i>Una vez se implemente y ponga en funcionamiento la solución FORTISIEM requerida por la ANM y que se instalará en la infraestructura tecnológica de la Agencia, el</i>	
---------	--	--



	<i>proveedor deberá realizar las configuraciones, integraciones y actividades de migración necesarias para continuar la prestación del servicio de monitoreo sobre dicha plataforma, garantizando la continuidad operativa, el monitoreo permanente y la correlación de eventos de seguridad, incluyendo la integración, normalización y correlación de las fuentes definidas por la ANM.</i>	
--	---	--

CUARTO: MODIFÍQUESE, el numeral 7.2.26 del Anexo de Especificaciones y Requerimientos Técnicos Mínimos conforme las descripciones y ajustes que se describen a continuación:

7.2.2.6	<i>El proveedor deberá garantizar que la solución SIEM este en capacidad de coleccionar, procesar, monitorear y correlacionar más de de 3000 EPS (Eventos por Segundo).sin filtrar y Filtrados 512 EPS</i>	
---------	--	--

QUINTO: MODIFÍQUESE, el numeral 7.6 del Anexo de Especificaciones y Requerimientos Técnicos Mínimos conforme las descripciones y ajustes que se describen a continuación:

7.6. RENOVIACION DE LICENCIAMIENTO VrX VICARUIS

La ANM requiere la renovación de licenciamiento y los servicios conexos la renovación de 150 licencias de VrX. por 12 meses, contados a partir de su activación. Con el siguiente alcance que incluya administración de plataforma y soporte de fabricante

Este producto debe ser licenciado a nombre de la Agencia Nacional de Minería.

VrX VICARUIS es plataforma SaaS unificada de gestión y remediación de vulnerabilidades que permite identificar, priorizar y corregir amenazas de ciberseguridad en tiempo real. Combina la detección de vulnerabilidades con herramientas activas como parches, scripts y "patchless protection" (protección sin parches) para proteger aplicaciones, sistemas operativos y software de terceros. Esta solución de gestión de vulnerabilidades es diseñada para ayudar a las organizaciones a identificar, priorizar y mitigar riesgos de seguridad en sus entornos tecnológicos de manera eficiente y automatizada. A diferencia de las herramientas tradicionales que se limitan a detectar vulnerabilidades, Vicarius incorpora capacidades avanzadas de remediación, incluyendo la aplicación de parches virtuales (virtual patching), lo que permite proteger sistemas incluso cuando no es posible aplicar actualizaciones oficiales de inmediato.

Entre sus principales características se destacan:

Descubrimiento y análisis continuo de vulnerabilidades: Monitorea activos en tiempo real para detectar exposiciones en sistemas operativos, aplicaciones y software de terceros.



Priorización inteligente de riesgos: Utiliza inteligencia contextual para clasificar vulnerabilidades según su nivel de criticidad, exposición y probabilidad de explotación.

Remediación automatizada: Permite aplicar soluciones correctivas de forma directa, reduciendo la dependencia de procesos manuales.

Patching sin interrupciones: A través de su enfoque de parcheo virtual, protege activos sin afectar la operación o disponibilidad de los sistemas.

Visibilidad centralizada: Ofrece paneles de control intuitivos que facilitan la toma de decisiones y el seguimiento del estado de seguridad.

Integración con herramientas existentes: Se adapta fácilmente a ecosistemas de TI ya implementados, optimizando los procesos de gestión de seguridad.

Con la firma del acta de inicio, el proveedor deberá presentar a la supervisión certificación vigente emitida por el fabricante Vicarius en la que se le haga constar su Calidad de partner o distribuidor autorizado de la mencionada Plataforma.

Los demás términos y condiciones no son objeto de modificación alguna y continúan vigentes y válidos.

Agradecemos su acostumbrada colaboración y gestión.

Atentamente,

ANDREA BIBIANA PEÑA GÓMEZ

Jefe Oficina de Tecnología e Información (E)

Anexos: 0

Copia: N/A

Elaboró: Sonia Catherine Ochoa Sanabria – Contratista OTI. *Sonia Ochoa S.*

Revisó: Luis Alonso Lugo Charry – Contratista OTI *L. Lugo*
Paolo Bonilla Rodríguez – Contratista OTI *P. Bonilla*

Fecha de elaboración: 15-10-2026 15:54 PM. *[Signature]*

Número de radicado que responde:

Tipo de respuesta: Total

Archivado en: Carpeta contractual