



OFICIO DE RESPUESTA A OBSERVACIONES

Bogotá D.C., septiembre de 2026

Señores
ON MOTION S.A.S.

Cordial saludo,

La Escuela Tecnológica Instituto Técnico Central agradece las observaciones presentadas dentro del proceso de Selección Abreviada de Menor Cuantía No. ITC-SAMC-013-2026, cuyo objeto es:

“CONTRATACIÓN DEL SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA LA MONITORIZACIÓN CONTINUA, ANÁLISIS, CORRELACIÓN, GESTIÓN Y RESPUESTA ANTE EVENTOS E INCIDENTES DE CIBERSEGURIDAD DE LA ETITC, INCLUYENDO LAS HERRAMIENTAS DE GESTIÓN Y ANÁLISIS NECESARIAS PARA EL CUMPLIMIENTO DEL SERVICIO Y LA DISPOSICIÓN DE EQUIPO TÉCNICO IDÓNEO Y CAPACITADO”.

Una vez efectuado el análisis de las observaciones de carácter técnico presentadas, la Entidad se permite responder en los siguientes términos:

1. CARÁCTER TÉCNICO

Observación No. 1

¿Cuántos GB/día y EPS procesa actualmente SolarWinds SEM?

La información relacionada con EPS, volumen de eventos, volumen de logs, arquitectura de monitoreo y demás parámetros internos de operación de las herramientas de seguridad corresponde a información sensible de la infraestructura tecnológica institucional. Por razones de seguridad de la información, dicha información será suministrada únicamente al contratista adjudicatario durante la fase de empalme e implementación del servicio.

Observación No. 2

¿Cuántos activos y fuentes de logs estarán bajo monitoreo?

La Entidad ha publicado en el Anexo Técnico la relación general de activos que harán parte del alcance del servicio. Las cantidades específicas, configuraciones, integraciones y características técnicas detalladas serán suministradas al contratista adjudicatario durante la fase de inicio del contrato.

CLASIF. DE CONFIDENCIALIDAD	IPB	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
-----------------------------	-----	-----------------------	---	---------------------------	---



Observación No. 3

¿SolarWinds SEM se encuentra implementado e integrado?

Sí, La ETITC cuenta actualmente con las plataformas SolarWinds Security Event Manager (SEM) y LevelBlue USM Anywhere, las cuales forman parte de la infraestructura tecnológica institucional. Corresponderá al proveedor adjudicatario realizar las actividades de ajuste, optimización, afinamiento e integración que resulten necesarias para la correcta prestación del servicio SOC.

Observación No. 4

¿La operación 7x24 puede prestarse desde un SOC compartido?

Sí, La Entidad no exige una dedicación exclusiva de infraestructura para la ETITC. Sin embargo, el proveedor deberá garantizar el cumplimiento permanente de los ANS, tiempos de respuesta, monitoreo continuo, escalamiento y atención de incidentes establecidos en el proceso contractual.

Observación No. 5

¿Los tres profesionales mínimos requieren dedicación exclusiva o presencialidad?

No se exige dedicación exclusiva. La prestación del servicio podrá realizarse de manera remota o presencial según la criticidad del incidente o requerimiento. No obstante, el contratista deberá garantizar la disponibilidad efectiva del personal ofertado durante toda la ejecución contractual y el cumplimiento de los niveles de servicio establecidos

Observación No. 6

¿Los ANS corresponden a atención o a solución definitiva?

Los ANS definidos corresponden a los tiempos máximos de identificación, análisis inicial, confirmación, escalamiento, notificación e inicio de acciones de respuesta. La recuperación total del servicio y la erradicación avanzada continuarán siendo responsabilidad de la ETITC dentro del esquema de responsabilidad compartida definido en el Anexo Técnico.

Observación No. 7

¿Las cantidades de pentesting, phishing y vishing constituyen bolsa o mínimos obligatorios?

Las capacidades indicadas corresponden a los mínimos requeridos por la Entidad durante la vigencia contractual. La programación específica de las actividades se ejecutará de acuerdo con las necesidades institucionales y el plan de trabajo aprobado por la supervisión.

CLASIF. DE CONFIDENCIALIDAD	IPB	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
-----------------------------	-----	-----------------------	---	---------------------------	---



Observación No. 8

¿La plataforma web integral del SOC debe ser suministrada por el contratista y cuántos usuarios accederán a ella?

La plataforma deberá ser suministrada por el contratista como parte integral de la prestación del servicio. La Entidad mantiene el requisito de usuarios y grupos ilimitados con el fin de garantizar acceso institucional permanente a la información generada durante la ejecución contractual.

Observación No. 9

¿El proveedor debe suministrar licenciamientos adicionales?

La ETITC suministrará las herramientas tecnológicas institucionales expresamente relacionadas en el Anexo Técnico. No obstante, el proveedor deberá incluir dentro de su propuesta todas aquellas herramientas, recursos, capacidades técnicas o licenciamientos complementarios que considere necesarios para cumplir integralmente con el objeto contractual y los requisitos técnicos definidos por la Entidad.

Observación No. 10

¿Qué herramientas deberán ser suministradas por el contratista?

El proveedor deberá suministrar, como mínimo:

- La plataforma integral de gestión de incidentes requerida en el numeral 1.2 del Anexo Técnico.
- Las herramientas necesarias para análisis de vulnerabilidades.
- Las herramientas necesarias para pruebas de penetración.
- Las plataformas y capacidades requeridas para campañas de phishing y vishing.
- Los mecanismos de Threat Hunting y Threat Intelligence que hagan parte del servicio ofertado.

Las herramientas actualmente relacionadas como propiedad de la ETITC continuarán siendo suministradas por la Entidad.

2) OBSERVACIONES ASPECTOS HABILITANTES

De conformidad con la observación no se acepta y se establece que los códigos solicitados son los que corresponden para garantizar la necesidad de la entidad.



PERSONAL MINIMO REQUERIDO HABILITANTE **Ingeniero de Ciberseguridad**

La Entidad se encuentra revisando y analizando las observaciones presentadas respecto de los perfiles profesionales, formación académica, experiencia y certificaciones exigidas para el personal mínimo requerido.

Una vez finalizado el análisis técnico y jurídico correspondiente, la Entidad determinará la procedencia de los ajustes que eventualmente resulten pertinentes, siempre que dichos cambios contribuyan a fortalecer el proceso de selección, promover una mayor participación de oferentes y mantener el nivel técnico requerido para la adecuada prestación del servicio SOC y el cumplimiento de las necesidades institucionales.

Lo anterior, se ajustara en el pliego de condiciones definitivo de acuerdo a lo aceptado y a la vez requerido por la Entidad.

Atentamente,

ESCUELA TECNOLÓGICA INSTITUTO TÉCNICO CENTRAL