



OFICIO DE RESPUESTA A OBSERVACIONES

Bogotá D.C., septiembre de 2026

Señores
IDENTIAN

Cordial saludo,

La Escuela Tecnológica Instituto Técnico Central, en atención a las observaciones presentadas dentro del proceso de Selección Abreviada de Menor Cuantía No. ITC-SAMC-013-2026, cuyo objeto es la “Contratación del servicio de Centro de Operaciones de Seguridad (SOC) para la monitorización continua, análisis, correlación, gestión y respuesta ante eventos e incidentes de seguridad de la información de la ETITC”, se permite dar respuesta en los siguientes términos:

Observación No. 1

Dimensionamiento de fuentes para el SIEM

Respuesta de la Entidad

La Entidad informa que en el documento de especificaciones técnicas se describen los activos tecnológicos que forman parte del alcance del servicio SOC. No obstante, las cantidades específicas, configuraciones, capacidades operativas y demás características detalladas de la infraestructura tecnológica serán suministradas al contratista adjudicatario durante la etapa de inicio del contrato y transferencia de conocimiento.

Lo anterior obedece a criterios de protección de la infraestructura tecnológica institucional y de seguridad de la información, evitando la divulgación pública de información sensible relacionada con la arquitectura de monitoreo y seguridad de la ETITC.

Observación No. 2

Provisión del licenciamiento del SIEM

Respuesta de la Entidad

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



La Entidad aclara que el licenciamiento de las herramientas de correlación y monitoreo actualmente implementadas se encuentra a cargo de la ETITC.

Dentro del alcance del servicio serán suministradas al contratista adjudicatario las plataformas de monitoreo y correlación disponibles, incluyendo las herramientas de seguridad indicadas en el anexo técnico. El proveedor deberá prestar el servicio SOC utilizando dichas herramientas y las capacidades técnicas complementarias que considere necesarias para el cumplimiento de las obligaciones contractuales.

Observación No. 3

Fabricante del SIEM

Respuesta de la Entidad

Actualmente la ETITC dispone de las siguientes plataformas de correlación y monitoreo:

SolarWinds Security Event Manager (SEM) versión 2025.4.
LevelBlue USM Anywhere Standard.

Los detalles de configuración, integración y operación serán suministrados al contratista adjudicatario durante la fase de implementación y empalme del servicio.

Observación No. 4

Alcance de las pruebas de ingeniería social

Respuesta de la Entidad

La Entidad aclara que las cantidades establecidas corresponden a usuarios objetivo y no a campañas independientes.

En consecuencia:

Hasta cien (100) pruebas de phishing corresponden a usuarios objetivo.
Hasta cincuenta (50) pruebas de vishing corresponden a usuarios objetivo.

La distribución de dichas actividades podrá realizarse mediante una o varias campañas de acuerdo con el plan de trabajo definido durante la ejecución del contrato y las necesidades institucionales identificadas por la ETITC.

Observación No. 5

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



Herramientas para ethical hacking y análisis de vulnerabilidades

Respuesta de la Entidad

Se aclara que las actividades de análisis de vulnerabilidades, pruebas de penetración tipo caja negra y caja blanca forman parte del alcance integral del servicio contratado.

En consecuencia, el proveedor deberá incluir dentro de su propuesta todas las herramientas, licenciamientos, recursos técnicos y especializados necesarios para la ejecución de estas actividades, de conformidad con los requerimientos establecidos en el anexo técnico.

Atentamente,

ESCUELA TECNOLÓGICA INSTITUTO TÉCNICO CENTRAL