



OFICIO DE RESPUESTA A OBSERVACIONES

Bogotá D.C., septiembre de 2026

Señores
LICETHREY

Referencia: Observaciones al proceso de Selección Abreviada de Menor Cuantía No. ITC-SAMC-013-2026.
Cordial saludo:

La Escuela Tecnológica Instituto Técnico Central agradece las observaciones formuladas al proceso cuyo objeto corresponde a 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 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 revisadas las observaciones de carácter técnico, la Entidad se permite responder en los siguientes términos:

OBSERVACIÓN 1 **Infraestructura, EPS, GB/día y dimensionamiento de la plataforma**

La Entidad ha publicado dentro del Anexo Técnico el alcance general de los activos tecnológicos que harán parte del servicio SOC. Sin embargo, la información relacionada con volumen de eventos (EPS), almacenamiento diario de registros, cantidad exacta de activos monitoreados, configuraciones internas, reglas de correlación, capacidad de procesamiento y demás elementos asociados a la arquitectura de seguridad institucional constituye información sensible de la infraestructura tecnológica de la ETITC.

Por razones de seguridad de la información, dicha información será suministrada exclusivamente al contratista adjudicatario durante la fase de empalme e implementación del servicio.

OBSERVACIÓN 2 **Plataforma SIEM y herramientas para la prestación del servicio**



La ETITC dispone actualmente de herramientas institucionales de monitoreo y correlación de eventos, las cuales serán suministradas al proveedor adjudicatario para la ejecución de las actividades propias del servicio SOC. No obstante, las herramientas complementarias requeridas para la prestación integral del servicio, incluyendo la plataforma web de gestión de incidentes, herramientas de análisis de vulnerabilidades, pruebas de penetración, phishing, vishing, threat hunting o capacidades adicionales que el oferente considere necesarias para garantizar el cumplimiento del objeto contractual, deberán ser suministradas por el contratista dentro de su propuesta técnica y económica.

OBSERVACIÓN 3 **Herramienta principal para la operación del SOC**

La ETITC cuenta actualmente con las plataformas:

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

Estas herramientas hacen parte de la infraestructura tecnológica institucional y estarán disponibles para la operación del servicio.

Corresponderá al proveedor adjudicatario realizar las actividades de monitoreo, correlación, gestión, parametrización, ajuste de reglas, optimización de detección y fortalecimiento continuo del servicio sobre las plataformas suministradas por la Entidad, así como integrar los componentes adicionales que resulten necesarios para el cumplimiento del alcance contractual.

OBSERVACIÓN 4 **Inconsistencia entre plazo contractual y formato económico**

La Entidad revisará la coherencia entre las cantidades reflejadas en el formato económico y el plazo de ejecución definido para el proceso, con el fin de realizar los ajustes documentales que resulten procedentes y evitar interpretaciones diferentes durante la presentación y evaluación de las ofertas.

OBSERVACIÓN 5 **Actividades con periodicidades semestrales o anuales** **Respuesta de la Entidad**

La ETITC aclara que para el presente proceso deberán ejecutarse las actividades específicamente requeridas dentro del plazo contractual definido. En consecuencia, cuando existan referencias a frecuencias generales de carácter anual o semestral, prevalecerán las cantidades mínimas



expresamente definidas en las especificaciones técnicas para la vigencia del contrato.

Las aclaraciones correspondientes serán incorporadas en la documentación definitiva cuando resulte necesario.

OBSERVACIÓN 6

Alcance de solicitudes de análisis de vulnerabilidades

Respuesta de la Entidad

La Entidad aclara que una solicitud podrá corresponder a uno o varios activos tecnológicos, aplicaciones, servidores, direcciones IP o servicios que requieran evaluación de seguridad.

Las actividades definidas constituyen capacidades mínimas que deberán estar disponibles durante toda la vigencia contractual y serán utilizadas de acuerdo con las necesidades identificadas por la ETITC durante la ejecución del contrato.

OBSERVACIÓN 7

Alcance de pruebas de penetración Black Box

Respuesta de la Entidad

La Entidad aclara que el alcance específico de cada ejercicio de Pentesting será definido durante la ejecución del contrato mediante solicitud formal.

Cada actividad podrá estar asociada a servidores, aplicaciones web, APIs, direcciones IP, servicios publicados o componentes tecnológicos que requieran validación, de acuerdo con las necesidades institucionales identificadas.

OBSERVACIÓN 8

Alcance de pruebas de penetración White Box

Respuesta de la Entidad

La Entidad aclara que las pruebas White Box podrán involucrar aplicaciones, APIs, componentes funcionales, credenciales de prueba, perfiles de usuario o información técnica que resulte necesaria para el alcance de la evaluación, conforme a las autorizaciones y condiciones definidas para cada solicitud específica.

OBSERVACIÓN 9

Tiempos de atención para vulnerabilidades y Pentesting

Respuesta de la Entidad

La Entidad aclara que los tiempos definidos en las especificaciones técnicas corresponden a los compromisos de atención y entrega de resultados asociados a las solicitudes formuladas por la ETITC.



Cada actividad incluirá recepción, validación, ejecución técnica, análisis y entrega de resultados, sin perjuicio de actividades posteriores de validación o seguimiento que puedan requerirse según la naturaleza de los hallazgos identificados.

OBSERVACIÓN 10

Disponibilidad del servicio SOC

Respuesta de la Entidad

La ETITC revisará la armonización de los diferentes porcentajes de disponibilidad contenidos en los documentos del proceso con el fin de garantizar consistencia documental y evitar interpretaciones ambiguas. Las precisiones correspondientes serán incorporadas mediante los mecanismos definidos para el proceso contractual.

OBSERVACIÓN 11

Relación entre ANS y matriz de criticidad

Respuesta de la Entidad

La Entidad aclara que los tiempos y ANS definidos en el proceso están orientados a medir actividades diferenciadas dentro del ciclo de gestión de incidentes, incluyendo detección, validación, escalamiento, notificación e inicio de acciones de contención. No obstante, se revisará la armonización documental correspondiente para facilitar su interpretación y aplicación durante la ejecución del contrato.

OBSERVACIÓN 12

Alcance del contratista posterior a la contención

Respuesta de la Entidad

La prestación del servicio opera bajo el modelo de responsabilidad compartida descrito en las especificaciones técnicas. En consecuencia:

El contratista será responsable de la detección, análisis, clasificación, notificación, escalamiento, acompañamiento técnico y contención de primer nivel.

La ETITC mantendrá la responsabilidad por las actividades de recuperación definitiva, restauración de servicios, recuperación operativa y toma de decisiones estratégicas relacionadas con el negocio.

Lo anterior sin perjuicio del acompañamiento técnico especializado que deberá prestar el proveedor durante toda la gestión del incidente.



OBSERVACIÓN 13

Bolsa de 40 horas especializadas

Respuesta de la Entidad

La bolsa de cuarenta (40) horas corresponde al total disponible durante la ejecución contractual y constituye un recurso adicional a las actividades ordinarias del servicio SOC.

Las horas podrán utilizarse para:

Atención especializada de incidentes.

Análisis técnico avanzado.

Apoyo especializado para contención.

Actividades de acompañamiento técnico definidas por la supervisión.

Su utilización deberá ser previamente coordinada y autorizada por el supervisor del contrato. Estas horas no reemplazan las obligaciones ordinarias asociadas al monitoreo continuo y la operación normal del SOC.

OBSERVACIÓN 14

Sustitución de ISO/IEC 25001 por ISO/IEC 27017

Respuesta de la Entidad

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.

OBSERVACIÓN 15

Límite de crecimiento de activos monitoreados

Respuesta de la Entidad

La Entidad informa que los activos descritos en las especificaciones técnicas constituyen la base de operación del servicio.

La incorporación de activos adicionales durante la ejecución contractual podrá presentarse en función de las necesidades institucionales y del crecimiento natural de la infraestructura tecnológica de la ETITC.

En caso de requerirse ampliaciones sustanciales que modifiquen de forma significativa el alcance inicialmente previsto, la Entidad evaluará las acciones contractuales correspondientes conforme a la normativa vigente.



OBSERVACIÓN 16

Retención de logs y almacenamiento

Respuesta de la Entidad

La información relacionada con retención específica de registros, volumen de logs, arquitectura de almacenamiento, capacidades de repositorios y demás características internas de la infraestructura tecnológica institucional constituye información sensible y será suministrada al contratista adjudicatario durante la etapa de implementación únicamente en la medida necesaria para la adecuada prestación del servicio.

OBSERVACIÓN 17

Inicio de monitoreo 7x24 frente al periodo de implementación

Respuesta de la Entidad

La ETITC aclara que el periodo de implementación hace parte integral del plazo contractual.

Durante dicha fase el contratista deberá ejecutar las actividades de despliegue, integración, configuración y puesta en operación definidas en el Anexo Técnico, garantizando el avance progresivo hacia la operación plena del servicio.

La ejecución de las actividades de monitoreo y operación deberá realizarse conforme al cronograma aprobado dentro del plan de trabajo y los hitos definidos juntamente con la supervisión del contrato

La Entidad agradece el interés y las observaciones presentadas, las cuales contribuyen al fortalecimiento del proceso de selección y a la adecuada estructuración contractual del servicio requerido.

Atentamente,

ESCUELA TECNOLÓGICA INSTITUTO TÉCNICO CENTRAL – ETITC