

Bogotá D.C., 8 de septiembre de 2026

Señores

Escuela Tecnológica Instituto Técnico Central – ETITC

Ciudad

Asunto: Observaciones al Proyecto de Pliego de Condiciones – Proceso ITC-SAMC-013-2026

Respetados señores:

En atención al Proyecto de Pliego de Condiciones del proceso ITC-SAMC-013-2026, 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, nos permitimos presentar las siguientes observaciones a los requisitos técnicos y factores de calidad.

Nuestro propósito es que los requisitos exigidos guarden relación directa con el objeto y con las actividades que efectivamente serán desarrolladas durante la ejecución del contrato.

1. El proyecto de pliego contempla dentro del factor de calidad las certificaciones ISO 25001, ISO/IEC 20000-1, ISO/IEC 27001 e ISO/IEC 27035.

Consideramos necesario revisar su pertinencia frente al objeto específico del proceso.

ISO 25001: solicitamos retirar este requisito, toda vez que su alcance incluye ingeniería de software y almacenamiento de datos, actividades que no corresponden al objeto del servicio SOC.

ISO/IEC 20000-1: solicitamos retirar este requisito y considerar en su lugar la ISO 9001, por cuanto el objeto corresponde a la prestación de un servicio especializado de SOC y no a la gestión integral de servicios de TI.

ISO/IEC 27001: solicitamos mantener y fortalecer este requisito, por ser el que guarda relación directa con el objeto de seguridad de la información y operación del SOC.

ISO/IEC 27035: solicitamos retirar este requisito, teniendo en cuenta que corresponde a una guía para la gestión de incidentes de seguridad de la información, no certificable a nivel organizacional, cuyos lineamientos se implementan e incorporan en la ISO/IEC 27001.

En consecuencia, proponemos que el componente de certificaciones se concentre en ISO 9001 e ISO/IEC 27001, fortaleciendo especialmente esta última en lo relacionado con seguridad de la información, ciberseguridad y operación SOC.

2. El proyecto contempla dentro del personal mínimo requerido un profesional en Ingeniería Electrónica, Ingeniería de Telecomunicaciones o áreas afines, con experiencia relacionada con redes, cableado estructurado, seguridad informática e IPv6.

Solicitamos revisar la pertinencia de este perfil frente al objeto contractual, toda vez que las actividades principales corresponden a monitoreo, análisis, correlación, gestión y respuesta ante eventos e incidentes de ciberseguridad.

En consecuencia, consideramos más pertinente que el personal mínimo requerido priorice los perfiles directamente asociados a la operación del SOC, particularmente los Analistas SOC Nivel 1 y Nivel 2, responsables de las actividades de monitoreo, análisis y gestión de incidentes.

Por lo anterior, solicitamos incorporar los perfiles de Analista SOC Nivel 1 y Nivel 2 dentro del personal mínimo requerido y revisar la necesidad de establecer como obligatorio el perfil relacionado con redes, de acuerdo con las actividades efectivamente previstas en el objeto contractual.

3. El proyecto asigna cuarenta (40) puntos al factor de calidad, distribuidos en diez (10) puntos por cada una de las certificaciones contempladas.

Consideramos que esta distribución debería revisarse, de manera que el puntaje permita valorar también las capacidades efectivas de operación del SOC.

Por lo anterior, solicitamos que parte del puntaje sea asignado a criterios directamente relacionados con la prestación del servicio, tales como:

- Disponibilidad y operación 7x24.
- Tiempos de detección y respuesta (MTTD y MTTR).
- Threat Hunting.
- SOAR y automatización.
- Continuidad y redundancia del SOC.

De esta manera, el factor de calidad permitirá ponderar tanto las certificaciones pertinentes como las capacidades técnicas y operativas que impactan directamente la prestación del servicio.

Con fundamento en las anteriores observaciones, solicitamos respetuosamente a la Entidad revisar y ajustar el Proyecto de Pliego de Condiciones en los aspectos señalados,

procurando que los requisitos técnicos, el personal mínimo y los factores de evaluación guarden relación directa con el objeto y las actividades propias del servicio de Centro de Operaciones de Seguridad (SOC).

Agradecemos a la Entidad el análisis de las observaciones presentadas y esperamos que sean tenidas en cuenta en la estructuración definitiva del proceso.