

INVITACIÓN PÚBLICA No. 002-2026
ADENDA No. 1 A LA INVITACIÓN

OBJETO: PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE SISTEMA DE GESTIÓN DE EVENTOS DE INFORMACIÓN DE SEGURIDAD (SIEM+SOC), PROTECCIÓN DE MARCA, GESTIÓN DE VULNERABILIDAD, SIMULACRO DE ATAQUES, CULTURA Y SENSIBILIZACIÓN.

En Cartagena de Indias D.T. y C., a los veintiocho (28) días del mes de abril de 2026, **MUTUAL SER EPS**, en uso de sus facultades legales, estatutarias y las establecidas en el Documento de Negociación, procede a expedir la presente Adenda, previas las siguientes:

CONSIDERACIONES

1. Que MUTUAL SER EPS dio apertura al proceso de selección de la referencia mediante la publicación del Documento de Negociación correspondiente.
2. Que, de conformidad con el cronograma del proceso, se habilitó la etapa de recepción de preguntas y observaciones por parte de los interesados.
3. Que dentro del plazo establecido se recibieron observaciones de los proponentes solicitando mayor claridad y precisión en la forma en que se asignarán los puntajes correspondientes al "Factor Calidad" (Calificación Técnica).
4. Que, en aras de garantizar los principios de transparencia, selección objetiva, igualdad de oportunidades y pluralidad de oferentes, MUTUAL SER EPS ha encontrado pertinente acoger las observaciones presentadas y, en consecuencia, procede a detallar y reestructurar algunos de los ítems 1 y 3 de los subfactores de calidad.

Por lo anteriormente expuesto, MUTUAL SER EPS,

RESUELVE:

ARTÍCULO PRIMERO. - MODIFICAR el numeral **3.1.1.2. FACTOR CALIDAD - CALIFICACIÓN TÉCNICA (HASTA 60 PUNTOS)** del Documento de Negociación, el cual quedará así:

3.1.1.1.2. FACTOR CALIDAD - CALIFICACIÓN TÉCNICA (HASTA 60 PUNTOS)

La calificación técnica tendrá un puntaje máximo de sesenta (60) puntos y evaluará la capacidad, idoneidad y madurez del proponente para la prestación del servicio.

Se dará especial relevancia a la capacidad de gestión, procesamiento y almacenamiento de grandes volúmenes de eventos de seguridad (logs), así como a la escalabilidad del servicio sin restricciones por ingesta de datos.

Asimismo, se evaluarán el modelo de operación del SOC, la gestión de incidentes, los niveles de servicio, las certificaciones del proponente y su equipo de trabajo, y el valor agregado ofrecido.

La calificación se realizará conforme a los siguientes criterios:

Ítem	Factor de Evaluación	Descripción	Escala de Evaluación	Soportes Requeridos	Puntaje Máximo
1	Operación SIEM sin restricción de ingesta	Se evaluará el modelo de licenciamiento de la plataforma SIEM propuesta, priorizando aquellas soluciones que garanticen una escalabilidad y operación sin restricciones por volumen de almacenamiento o límite de Eventos Por Segundo (EPS).	9 puntos: Ofrece un modelo basado en volumen de almacenamiento o EPS, garantizando la operación del servicio sin afectaciones. Sin limitación de volumen. 0 puntos: Ofrece un modelo basado en volumen de almacenamiento o EPS que cumple con la operación del servicio, con restricción por volumen de logs.	Propuesta técnica detallada y declaración del fabricante sobre el modelo de licenciamiento.	9
2	Servicio SOC (modelo operativo)	Se evaluará la madurez del modelo SOC, incluyendo metodologías adoptadas (NIST, MITRE ATT&CK), capacidades de Threat Hunting, automatización mediante SOAR, estructura del equipo y nivel de cobertura operativa del servicio.	8 puntos: Demuestra integración nativa de plataforma SOAR con ejecución de Playbooks automatizados y mapeo del framework mitre att&ck 4 puntos: SOC estándar con procesos de análisis de escalamiento manuales	Flujogramas técnicos de los Playbooks y arquitectura funcional propuesta.	8
3	Gestión de incidentes 7x24 y Forense Digital	Se evaluará de forma competitiva la agilidad en el tiempo de contención activa de incidentes críticos. Se otorgará el puntaje máximo a	Al proponente que ofrezca el menor tiempo garantizado (expresado en minutos exactos) para	Declaración técnica firmada donde el oferente estipule su compromiso de tiempo de contención	7

Ítem	Factor de Evaluación	Descripción	Escala de Evaluación	Soportes Requeridos	Puntaje Máximo
		la oferta que presente el menor tiempo de contención garantizado frente a los demás competidores, siempre y cuando acredite tener forense propio.	la contención activa de incidentes frente a todas las demás propuestas habilitadas, y que acredite contar con equipo forense digital especializado de planta (in-house). (Nota: Si dos o más proponentes empatan ofreciendo el mismo menor tiempo, se les otorgarán los 7 puntos a todos los empatados) 0 Puntos: A los proponentes que ofrezcan tiempos de contención superiores al menor tiempo ofertado en el proceso, a quienes no expresen su tiempo en minutos exactos, o cuyo equipo forense sea tercerizado/bajo demanda.	exacta en minutos, junto con la relación/hojas de vida del equipo forense in-house.	
4	Gestión de vulnerabilidades	Se evaluará el alcance del servicio, periodicidad de escaneos, metodología de priorización de vulnerabilidades (riesgo/criticidad), seguimiento a la remediación y calidad de los informes generados.	6 puntos: Plataforma con escaneo continuo/diario y priorización basada en riesgo de negocio real. 3 Puntos: Metodología basada únicamente en escaneos programados mensuales o trimestrales.	Ficha técnica de la solución de vulnerabilidades propuesta.	6
5	Protección de marca	Se evaluará la capacidad	4 Puntos: Monitoreo	Ficha técnica o	4

Ítem	Factor de Evaluación	Descripción	Escala de Evaluación	Soportes Requeridos	Puntaje Máximo
		para monitorear activos digitales (dominios, redes sociales, identidades), detectar suplantaciones, gestionar procesos de takedown y generar análisis de riesgos digitales.	que incluye web superficial, Deep Web, Dark Web y takedown (desmante) automatizado. 2 Puntos: Monitoreo limitado a web superficial y redes sociales sin takedown automático.	descripción funcional de la herramienta de Brand Protection.	
6	Simulacros de ataque	Se evaluará la ejecución de ejercicios de seguridad tipo Red Team, Purple Team y mesas de crisis, incluyendo metodología aplicada, frecuencia, alcance y generación de lecciones aprendidas.	4 Puntos: Simulacros bajo metodología Red Team / Purple Team, incluyendo mesas de crisis con la Gerencia/Junta. 2 Puntos: Simulacro técnico tradicional limitado a infraestructura y sin mesa de crisis.	Metodología detallada de ejecución de los simulacros.	4
7	Cultura organizacional + phishing	Se evaluará la estrategia de concientización en ciberseguridad, campañas de phishing, medición de resultados (indicadores de madurez) y fortalecimiento del comportamiento del usuario.	3 Puntos: Plataforma con campañas gamificadas, orientadas por roles y medición del nivel de madurez del usuario. 1 Punto: Servicio limitado al envío masivo de correos falsos (phishing estándar).	Alcance y/o demo funcional de la plataforma de concienciación.	3
8	ANS con el proveedor	Se evaluará la definición de acuerdos de nivel de servicio (SLA), tiempos de respuesta, indicadores de cumplimiento (KPI), mecanismos de seguimiento y esquema de penalidades.	3 Puntos: Propone un esquema de compensación o penalidades económicas a favor de MUTUAL SER EPS por incumplimiento de los ANS.	Matriz de Niveles de Servicio y propuesta de compensaciones o descuentos aplicables.	3

Ítem	Factor de Evaluación	Descripción	Escala de Evaluación	Soportes Requeridos	Puntaje Máximo
			0 Puntos: Solo se limita a cumplir los ANS mínimos sin compensación adicional.		
9	Inteligencia de amenazas (Threat Intelligence)	Se evaluará el uso de fuentes de inteligencia, integración de indicadores de compromiso (IoC), correlación de amenazas, análisis proactivo y capacidad de anticipación frente a riesgos emergentes.	3 Puntos: Integración de fuentes externas (IoC) alimentadas por bases de datos exclusivas de ciberataques en el sector salud. 1 Punto: Inteligencia de amenazas genérica sin enfoque sectorial.	Evidencia de suscripción o integración de feeds de IoCs en salud.	3
10	Reportes, dashboards y gobierno del servicio	Se evaluará la generación de informes técnicos y ejecutivos, dashboards de visibilidad, definición de indicadores de seguridad, realización de comités de seguimiento y trazabilidad del servicio.	3 Puntos: Acceso a un portal web en tiempo real (dashboard interactivo) con 100% de visibilidad de eventos y ANS. 1 Punto: Entregables limitados a reportes en PDF o Excel de forma mensual.	Descripción de la interfaz o portal de cliente dentro de la propuesta.	3
11	Certificaciones de la empresa	Se evaluará la existencia de certificaciones vigentes del proveedor (ej. ISO 27001, ISO 20000 u otras relacionadas), que evidencien la madurez de sus procesos y su sistema de gestión de seguridad de la información.	5 Puntos: Acredita ISO 20000 o ISO 22301 adicional a la ISO 27001, entre otras. 0 Puntos: Acredita únicamente la ISO 27001 (la cual ya se validó como requisito mínimo habilitante).	Copia de las certificaciones internacionales adicionales vigentes.	5
12	Certificaciones del personal	Se evaluará la idoneidad del equipo de trabajo mediante	5 Puntos: El equipo asignado supera el	Copia de los certificados técnicos y	5

Ítem	Factor de Evaluación	Descripción	Escala de Evaluación	Soportes Requeridos	Puntaje Máximo
		certificaciones técnicas (ej. CISSP, CISM, CEH, Security+), experiencia comprobada y asignación de roles especializados dentro del SOC.	perfil mínimo al contar con al menos tres (3) certificaciones globales elite (ej. CISSP, CISM, GCFA, OSCP). 0 Puntos: El personal solo cumple con los diplomas/certificados mínimos exigidos.	profesionales adicionales del personal propuesto.	
	TOTAL				60

ARTÍCULO SEGUNDO. - ALCANCE DE LA ADENDA: Las modificaciones introducidas mediante la presente Adenda prevalecerán sobre cualquier disposición en contrario contenida en el Documento de Negociación original o en sus anexos.

ARTÍCULO TERCERO. - VIGENCIA DE LAS DEMÁS CONDICIONES: Todos los demás numerales, condiciones, anexos y especificaciones del Documento de Negociación No. 002-2026 que no hayan sido expresamente modificados por la presente Adenda, permanecen incólumes y plenamente vigentes para todos los efectos del proceso de selección.