1. OBJETO

Contratar la renovación de licencias, mantenimientos preventivo, correctivo y soporte técnico para la plataforma de gestión de eventos e información de seguridad (SIEM – Security Information and Event Manager)

2. ALCANCE

Con el objeto descrito la SAE pretende contratar:

- Renovación de Licenciamiento asociado al SIEM
- Servicios de SOC y NOC
- Soporte técnico por un periodo de tres (3) años para la plataforma.
- Mantenimiento preventivo, el cual incluye afinamientos y actualización de la plataforma.
- Transferencia de conocimiento sobre la plataforma.

3. DETALLES TÉCNICOS

3.1 Renovación de las licencias del equipo SIEM

Se requiere la renovación de licenciamiento para el appliance virtual FortiSIEM con serial #FSMP000000002175 (derechos a actualización, soporte técnico de fabricante y corrección de fallas) por un periodo de 36 meses, el licenciamiento debe incluir.

- 175 dispositivos.
- 25 agentes avanzados

Nota: El oferente deberá garantizar que se entregue el licenciamiento requerido en el mismo esquema y alcance con el que actualmente cuenta la entidad

3.2 Mantenimiento preventivo

El contratista deberá realizar un (1) mantenimiento preventivo mensual durante la vigencia del contrato, este mantenimiento debe tener una duración mínima de 8 horas. Esta actividad debe incluir actualizaciones de versión de la solución, mantenimiento de espacios en disco, revisión de desempeño de la plataforma y afinamientos requeridos, cambios de componentes monitoreados, reconfiguraciones, mantenimiento proactivo.

El contratista deberá entregar el informe respectivo al Supervisor del Contrato a los cinco (5) días hábiles luego de cada mantenimiento, éste debe incluir las actividades realizadas, versiones iniciales y finales de SIEM, pruebas de verificaciones realizadas, resultado del afinamiento con

actividades, hallazgos, acciones realizadas para mejoramiento, y recomendaciones sobre la plataforma, de ser necesario se deben incluir planes de acción con actividades, fechas y responsabilidades específicas para la solución de los mismos.

Las actividades de mantenimiento preventivo y/o correctivas que se realicen sobre la solución deben ser coordinados previamente con el supervisor del contrato y después de la ejecución debe ser entregada la documentación correspondiente donde esté totalmente detalladas las actividades ejecutadas.

3.3 Servicios de NOC y SOC

Destinado al monitoreo de equipos y de red 7x24x365, con visibilidad en tiempo real de los incidentes en el desarrollo de la operación a través de la herramienta.

El contratista debe prestar el servicio de NOC y SOC remoto, 7*24 incluidos días festivos, con el fin de reportar las alertas generadas por la plataforma del SIEM. El NOC/SOC del contratista deberá conectarse a la plataforma instalada en la entidad mediante conexión VPN SSL suministrada por el firewall de la Entidad.

El contratista debe disponer de una línea telefónica para el reporte de los incidentes, los cuales también se podrán reportar a través de correo electrónico o vía internet.

El servicio de NOC/SOC debe incluir:

- Monitoreo de equipos y de red 7x24x365, con obtención de visibilidad en tiempo real de los incidentes en el desarrollo de la operación de la infraestructura monitoreada por el SIEM.
- Boletines de alertas y advertencias mensualmente
- Monitoreo y análisis de la información generada por los equipos de seguridad de la entidad con el fin de obtener alertas tempranas de posibles falencias o ataques de seguridad que se estén realizando a la entidad.

En el momento del reporte del incidente se deberá hacer un registro que incluya mínimo los datos de fecha, hora, descripción y numero del incidente. Dicho número servirá para identificar y hacer seguimiento del mismo.

3.4 Soporte técnico

El proveedor debe prestar el soporte técnico sobre la herramienta completa del SIEM, que incluya funcionalidades y configuración del SIEM, y el soporte sobre el software base de ésta (sistema operativo).
El proveedor debe prestar el soporte de forma telefónica, por correo o en sitio para la solución de consultas o incidentes sobre la operación, configuración o administración de la herramienta. La

entidad indicará la modalidad de atención requerida, de acuerdo con la naturaleza del requerimiento y a la criticidad de este.

3.4.1 Procedimiento de reporte de casos de soporte

A más tardar una semana después de la firma del acta de inicio el proveedor deberá suministrar la siguiente información:

a. Nivel de escalamiento, indicando:
   1. Nivel de escalamiento, por ejemplo: primer, segundo, tercer, etc.
   2. Rol responsable del escalamiento, por ejemplo: mesa de ayuda, coordinador de servicio, líder de servicio, etc.
   3. Datos de contacto del responsable del rol:
      - Nombre completo (nombre(s) y apellido(s)) del responsable.
      - Dirección de correo electrónico.
      - Número (s) de teléfono.

b. Para el reporte de los casos de soporte:
   1. Si se tiene habilitada una plataforma web, suministrar la URL del Help Desk y las credenciales asignadas a la SAE, junto con un manual de operación que describa la entrada al sistema; la forma de colocar una incidencia, anexar documentos, hacerle seguimiento y aceptar o rechazar su solución.
   2. Direcciones de correo electrónico de contacto.
   3. Números telefónicos fijos y celulares.
   4. Nombres de los ingenieros de soporte.

La SAE abrirá los casos de soporte en primera instancia en el Help Desk del proveedor vía web, en caso de estar habilitada; en segunda instancia, vía telefónica o email. El tiempo de atención para aplicación de los ANS empezará a contar desde el momento en que se produzca la solicitud y constituirán evidencia de ello: la fecha y hora de la generación del número de tiquete del Help Desk; o la fecha y la hora de la llamada; o la fecha y la hora del envío del email.

3.5 Transferencia de conocimiento en la gestión de la herramienta

El contratista deberá realizar una sesión de transferencia de conocimiento en la gestión de la herramienta, en la que se incluya conocimiento de la operación global de la herramienta, nuevas funcionalidades de la herramienta u optimizaciones de las funcionalidades de la misma, realizando énfasis en monitoreo de aplicaciones, desempeño de canales de comunicación, afinamientos a los eventos generados por la plataforma.

La sesión de transferencia de conocimiento deberá generarse con un tiempo mínimo de 4 horas de duración, independientes del tiempo solicitado como visitas mensuales.

Se deben realizar sesiones semestrales de transferencia de conocimiento, con mínimo 4 horas de duración, sobre nuevas funcionalidades liberadas para la herramientas y adopción de funcionalidades que la entidad solicite parala operación de la herramienta. Pudiéndose incluir en

las sesiones temas relacionados con riesgos de seguridad de la información a los que se pueda exponer la entidad en su operación, nuevas amenazas surgidas y mejores prácticas de seguridad aplicables a la entidad.

4. ACUERDOS DE NIVELES DE SERVICIOS

El tiempo máximo de atención se contará a partir del reporte del caso de soporte por parte de la Entidad, hasta (tiempo máximo) el inició de la atención del caso de forma presencial o remota por parte del proveedor.

El tiempo máximo de solución empezará a contar a partir del inicio de la atención mencionada y hace referencia al tiempo máximo del que dispone el proveedor para dar solución al caso y retornar a la operación normal el sistema.

Nivel de criticidad	Descripción	Tiempo máximo de atención	Tiempo máximo de solución	Disponibilidad de atención	Penalidad
Nivel 3 – Criticidad baja	Refiere incidentes que no afectan la disponibilidad de los servicios del SIEM y cumplimiento de los mantenimientos preventivos establecidos para el SIEM. Se aplicarán también para los casos de soporte que se generen por los medios descritos.	8 horas	24 horas	5x8	0.5% del valor total del contrato
Nivel 2 – Criticidad media	Refiere incidentes que afectan medianamente los servicios del SIEM (intermitencias), por ejemplo, incidentes que no permitan el monitoreo de algún componente.	4 horas	8 horas	5x8	1.0 % del valor total del contrato
Nivel 1 – Criticidad Alta	Refiere incidentes que afectan por completo la disponibilidad del servicio del SIEM	2 horas	4 horas	7x24	1.5% del valor total del contrato

La medición de los Acuerdo de Niveles de Servicio (ANS) anteriores se realizará de manera mensual, y para ello el CONTRATISTA deberá entregar al supervisor de contrato un informe de gestión mensual, en medio físico y magnético, dentro de los cinco (5) primeros días hábiles del mes después de la finalización de cada mes.

Luego de presentarse incumplimientos en los acuerdos de niveles de servicio (ANS) en más de tres (3) ocasiones acumuladas durante la vigencia del contrato, la Entidad podrá iniciar la aplicación de las garantías que se establezcan para el contrato.

En todo caso, para efectos de la aplicación de las sanciones previstas en este numeral se dará cumplimiento al procedimiento establecido en el artículo 86 de la Ley 1474 de 2011, en concordancia con el artículo 17 de la Ley 1150 de 2007.

5. CERTIFICACIÓN REQUERIDA

El Oferente debe proporcionar la certificación del fabricante del SIEM donde conste que es canal certificado en nivel Gold o Platino.

6. PROFESIONAL PARA SOPORTE TÉCNICO

El proponente debe garantizar el personal necesario para cumplir el objeto del contrato, el cual estará bajo cuenta y riesgo del contratista, entendiéndose que no se genera relación laboral alguna ni con el contratista ni con el personal a su cargo, en consecuencia, tampoco existirá pago de prestaciones sociales ni de ningún tipo de costos distintos al valor acordado, por parte de la Entidad.

Para garantizar la ejecución de las actividades asociadas con el soporte y mantenimiento del SIEM, el oferente deberá disponer cómo mínimo del siguiente profesional:

Cantidad	Rol a desempeñar	Formación Académica		Experiencia Específica	
		Pregrado	**Certificaciones**	**Especifica**	**Requerimiento particular**
1	Ingeniero de Soporte	Ingeniero de sistemas, Electrónico, de comunicaciones, Telemático, Ingeniero de redes.	Como mínimo debe contar con la Certificación NSE 5 de fortinet	Mínima de dos (2) años	Dos (2) años de experiencia en como ingeniero de soporte en la plataforma de SIEM.