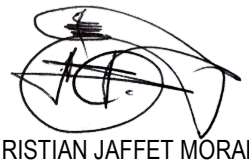
ANEXO TÉCNICO "RENOVACIÓN DEL SERVICIO DE RECOLECCIÓN, ALMACENAMIENTO Y CORRELACIÓN DE LOGS, CON CAPACIDAD DE ANÁLISIS BASADO EN COMPORTAMIENTO DE USUARIOS Y ENTIDADES Y RESPUESTA AUTOMATIZADA".

<table>
<tr><th colspan="5">ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS</th></tr>
<tr><td>1.</td><td colspan="4">Cantidad de suscripciones a renovar: 1 (Global) para una cantidad de 500 Gb diarias de ingesta de logs.
SaaS Cloud esscencial volum VESSB
SaaS Cloud esscencial volum VIRR</td></tr>
<tr><td>2.</td><td colspan="4">El contratista deberá prestar un servicio durante el periodo de vigencia del licenciamiento de la herramienta que incluya:
Soporte técnico y garantía por parte del contratista por el periodo del licenciamiento en un esquema 7 x 24 incluyendo acceso al portal de soporte, soporte a casos y recursos técnicos asociados.
Los incidentes técnicos podrán ser reportados vía web, chat y teléfono.
El contratista deberá garantizar la atención del servicio postventa y garantía para las plataformas en un esquema 7x24 por el periodo de licenciamiento.
El SERVICIO TECNICO debe incluir atención de incidentes sobre las plataformas ofertadas.
El SERVICIO TECNICO debe permitir consultas a través de llamadas telefónicas, correo electrónico.
El servicio técnico debe tener el alcance de integración y afinamiento de nuevas fuentes de logs con que cuente la Entidad.
Se deberá tener el alcance de realizar los parseos de logs que sean requeridos de acuerdo a las nuevas fuentes de logs que requiera la Entidad.
El contratista deberá garantizar que la Entidad siempre cuenta con las últimas versiones de la plataforma ofertada.
El SERVICIO TECNICO debe permitir sesiones remotas y atención de acuerdo con lo requerido por la supervisión del contrato, en caso de requerirse, en horario hábil y no hábil. Esto, con respecto a la plataforma ofertada y objeto del presente contrato.</td></tr>
<tr><td>3.</td><td colspan="4">Los siguientes son los términos de respuesta del SERVICIO TECNICO exigible al contratista:
<table>
<tr><th colspan="2">PRIORIDAD</th><th>DESCRIPCIÓN</th><th>TÉRMINO DE RESPUESTA</th></tr>
<tr><td>1</td><td>CRITICA</td><td>La producción esta parada o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia.</td><td>De manera remota o la indicada por el supervisor del contrato (2) horas.</td></tr>
<tr><td>2</td><td>ALTA</td><td>Experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida.</td><td>De manera remota o la indicada por el supervisor del contrato (4) horas.</td></tr>
<tr><td>3</td><td>MEDIA</td><td>Experimenta una pérdida de servicio menor, el impacto es un inconveniente.</td><td>De manera remota o la indicada por el supervisor del contrato (8) horas.</td></tr>
<tr><td>4</td><td>BAJA</td><td>No impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas.</td><td>De manera remota o la indicada por el supervisor del contrato (24) horas.</td></tr>
</table></td></tr>
<tr><td>4.</td><td colspan="4">El contratista deberá garantizar que se puedan escalar casos de soporte a la casa fabricante durante toda la vigencia del licenciamiento de la solución contratada.</td></tr>
<tr><td>5.</td><td colspan="4">El licenciamiento de esta suscripción deberá iniciar el día 15 de enero de 2024 y tener vigencia durante la cantidad de meses que serán contratados por la Entidad segun en el precio del servicio mensual ofertado por el oferente adjudicatario.</td></tr>
<tr><td>6.</td><td colspan="4">El contratista deberá realizar transferencia de conocimiento especializada en Analista de Operaciones de Seguridad SOC que incluya la certificación del personal. Esta transferencia de conocimiento se deberá entregar para al menos 02 (dos) miembros de la Entidad.</td></tr>
<tr><td>7.</td><td colspan="4">La entidad hace claridad en que la naturaleza de los datos serán propiedad de la misma (incluyendo registros y metadatos). Incluyendo cuando el fabricante esté sometido a normas extranjeras que permitan pedir información por parte de otras agencias o estados.</td></tr>
<tr><td>8.</td><td colspan="4">El contratista deberá garantizar que la portabilidad de los datos una vez finalizado el servicio, se haga mediante el formato de log en crudo o .RAW.</td></tr>
<tr><td>9.</td><td colspan="4">El contratista deberá entregar un certificado emitido por el fabricante donde certifique que se ha eliminado toda la información de la entidad, una vez finalizado el servicio contratado.</td></tr>
</table>

10.	El contratista deberá garantizar que, una vez finalizado el servicio, los datos de la entidad podrán ser portados a una infraestructura que la entidad designe, la cual podrá estar on premise o en nube. Si la entidad no cuenta con una plataforma para descargar esta información, deberá ser proveída por el contratista por un periodo de al menos 30 días. Este servicio y los trabajos asociados al proceso de transferencia de la información no deberán generar costos adicionales para la entidad.



Capitán KHRISTIAN JAFFET MORALES VARGAS
Comité Estructurador Técnico



Mayor ALEX RENÉ GUERRERO CRISTANCHO
Gerente de Proyecto