Superintendencia de Industria y Comercio

ANEXO No. 1B ESPECIFICACIONES TÉCNICAS – SOLUCION ANY.RUN INTELIGENCIA DE AMENAZAS (THREAT INTELLIGENCE) HUNTER

Las siguientes son las especificaciones técnicas mínimas que requiere la Entidad, para el cumplimiento del objeto contractual.

LAS ESPECIFICACIONES TÉCNICAS – FICHA TÉCNICA VAN DE ACUERDO CON LOS GRUPOS SEÑALADOS EN EL PLIEGO DE CONDICIONES

DENOMINACIÓN TÉCNICA: RENOVACIÓN DE SUSCRIPCIONES Y SOPORTE PARA LOS PRODUCTOS ANY.RUN INTELIGENCIA DE AMENAZAS (THREAT INTELLIGENCE)						
PLATAFORMA	**CLASIFICACIÓN DEL BIEN O SERVICIOS**	**PART NUMBER/SERIAL/SKU**	**DESCRIPCIÓN**	**CANTIDAD**	**UNIDAD**	**VENCIMIENTO**
ANY.RUN INTELIGENCIA DE AMENAZAS (THREAT INTELLIGENCE)	81111801 o 81112208 o 43233201 o 43233203 o 43233204 o 43233205	Asociado a Correo Electrónico	ANY.RUN INTELIGENCIA DE AMENAZAS (THREAT INTELLIGENCE) – SUSCRIPCIÓN HUNTER	1	SUSCRIPCIÓN	29/12/2026
No.	**OBLIGACIONES TÉCNICAS**					
1.	Permitir la consolidación de información sobre cualquier amenaza utilizando diferentes parámetros de búsqueda, incluidos nombres de amenazas, hashes de archivos, IPs, claves de registro y reglas YARA.					
2.	DOCUMENTO DE DERECHO DE USO Y VIGENCIA: En el momento de la entrega de los elementos objeto del contrato, el contratista debe entregar documento donde se acredite el derecho de uso y vigencia, licencias y renovaciones adquiridas, y de los de soporte y mantenimiento a nombre de la Superintendencia de Industria y Comercio. Este documento deberá identificar la suscripción adquirida, las fechas de inicio y finalización de su vigencia y las condiciones de soporte, mantenimiento y garantía aplicables durante el periodo contratado. Asimismo, el contratista deberá aportar la evidencia de activación de la suscripción en la plataforma del fabricante, para su verificación por parte de la supervisión del contrato.					
3.	Realizar inteligencia de amenazas en tiempo real impulsada por la comunidad de por lo menos 500.000 analistas a nivel mundial, y de incidentes o ataques cibernéticos, a partir de muestras nuevas cargadas en servicios o plataformas de sandbox.					
4.	Búsqueda de amenazas, por lo menos 500 búsquedas al mes.					
5.	Asumir los costos y demás gastos ocasionados con la entrega y traslados de las licencias objeto del contrato					
6.	Atender todas las solicitudes que hagan los supervisores, quienes informarán del funcionamiento defectuoso o la presencia de fallas de acceso, activación, funcionamiento o disponibilidad de las funcionalidades, durante toda la vigencia de la suscripción					
7.	La adquisición, renovación y/o actualización es por la vigencia de un (1) año, a partir de suscripción del acta de inicio del contrato y activación de los productos o mínimo a partir del día siguiente al vencimiento de la suscripción y en un término que no supere los 10 días hábiles					
8.	En caso de que las actualizaciones o cambios de versión realizados por el fabricante afecten las funcionalidades, configuraciones o condiciones de acceso utilizadas por la Entidad, el contratista deberá brindar el acompañamiento técnico necesario para identificar y gestionar dichas afectaciones, incluyendo el escalamiento al fabricante cuando corresponda. El contratista debe asegurar un plan de trabajo para ejecutar todas las actividades necesarias para que la transición entre versiones se realice sin que esto incurra en afectaciones o perdidas de información y de las funcionalidades actuales, así como preparar todas las contingencias y medidas de respaldo.					
9.	Acceso a soporte técnico especializado y actualizaciones periódicas del servicio, asegurando la adaptación a las nuevas amenazas y tendencias en ciberseguridad.					
10.	Efectuar la entrega de la documentación técnica de los bienes adquiridos al personal (técnico y funcional) de la SIC encargado de su funcionamiento y custodia					
11.	En el momento de la entrega y activación de los servicios objeto del contrato, el contratista debe entregar documento donde se acredite titularidad y vigencia, de la suscripción adquirida, y de los servicios de soporte y mantenimiento a nombre de la Superintendencia de Industria y Comercio, en donde relacione la vigencia del soporte y las garantías de la suscripción al licenciamiento adquirido.					
12.	El Contratista debe suministrar ocho (8) horas de transferencia de conocimientos, dentro de la cual se traten temas de instalación, configuración y nuevas funcionalidades de la plataforma para la SIC.					
13.	En caso de requerirse, el contratista con el apoyo del fabricante deberá realizar el afinamiento integral de las configuraciones, reglas y demás funcionalidades sobre la plataforma, bajo las buenas prácticas de industria, que le permitan a la Entidad optimizar y mejorar el rendimiento sobre la solución, con el personal especializado, capacitado y certificado					

	GARANTÍA
14.	Al momento de la entrega de las suscripciones, el contratista debe entregar una certificación donde se otorgue mínimo un (1) año de garantía del fabricante para las licencias de software. El contratista verificará y enviará a la SIC la documentación necesaria donde se evidencie que el licenciamiento quedó activo en el portal del fabricante.
15.	El contratista debe garantizar el cambio de las licencias por una nueva, de iguales o superiores características técnicas, cuando se presenten un número acumulado mayor a una (1) falla técnica, durante el tiempo de garantía, sin ningún tipo de costo para la entidad. Entendiéndose como falla, el no funcionamiento de cualquiera de los componentes del software.
16.	Una vez efectuada la entrega el contratista deberá explicar claramente la metodología que deberá seguir por la entidad para solicitar el servicio de garantía.
17.	Corregir las fallas en el servicio o en los bienes suministrados que resulten defectuosos dentro del plazo que le señale el supervisor del contrato.
18.	Garantizar la calidad y correcto funcionamiento de las licencias suministradas, durante el plazo de ejecución del contrato y la vigencia de las licencias adquiridas
19.	Realizar la entrega de nuevas actualizaciones sin costo durante el tiempo de garantía de las licencias.
	SOPORTE PARA SOFTWARE Y/O HARDWARE
20.	El contratista deberá suministrar el servicio de suscripción y soporte del fabricante del software y/o hardware durante un (1) año.
21.	Protección de la actualización del software sin costo alguno al acceso de nuevas versiones y mejoras durante un (1) año.
	TIPO DE LICENCIAMIENTO Y USUARIOS
22.	ANY.RUN Threat Intelligence – Core: corresponde a una suscripción anual para acceso a las capacidades de inteligencia de amenazas. El consumo se controla mediante la capacidad contratada para el equipo; actualmente el fabricante publica para Core hasta 25.000 solicitudes mensuales por equipo.
	COBRO POR CONSUMO O TARIFA PLANA
23.	ANY.RUN Threat Intelligence – Core – El licenciamiento corresponde a una suscripción por un (1) año bajo modalidad de tarifa plana, sin cobros adicionales asociados al consumo o uso de las funcionalidades contempladas en el plan contratado.
	SOPORTE, IDIOMA, TIEMPOS DE RESPUESTA Y DISPONIBILIDAD
24.	Por tratarse principalmente de herramientas especializadas para actividades de análisis de seguridad, inteligencia de amenazas, OSINT, monitoreo de marca y análisis forense, se requiere que durante toda la vigencia de las licencias exista soporte técnico del fabricante o del canal autorizado. Soporte durante la vigencia de la licencia, mediante correo electrónico, portal de soporte o chat, según corresponda al fabricante, atención en español o inglés, acceso a actualizaciones, correcciones y documentación, y escalamiento al fabricante cuando la solución presente fallas que impidan su utilización. Para las soluciones SaaS, el proveedor deberá informar las condiciones de disponibilidad del servicio y los tiempos de atención ofrecidos por el fabricante.
	HABILITACIÓN, CREDENCIALES, TRANSFERENCIA DE CONOCIMIENTO Y VERIFICACIÓN
25.	El proveedor deberá realizar o acompañar la renovación, habilitación y/o activación de cada una de las licencias y suscripciones, conservando cuando aplique las cuentas institucionales existentes, proyectos, configuraciones e información disponible. Deberá entregar las credenciales, códigos de licencia, accesos administrativos o mecanismos de activación que correspondan, verificar conjuntamente con la entidad y realizar una sesión de transferencia de conocimiento orientada principalmente a los cambios, nuevas funcionalidades, administración y condiciones de uso de las versiones renovadas. Verificación de la correcta activación de las licencias y de la disponibilidad de las funcionalidades, capacidades y límites correspondientes al plan contratado, dejando constancia de su habilitación.

Adriana Cetina Hernández
Jefe Oficina de Tecnología e Informática

Proyectó: Jeffer Ricardo Ruiz Leal – Contratista G. de Informática Forense y Seguridad Digital
Revisó: Magda Julieth Zarrate Saldaña - Coordinadora G. de Informática Forense y Seguridad Digital
Nelson Romero Muñoz– Contratista OTI.
Mauricio Salgado Guzman – Contratista OTI.
Aprobó: Adriana Cetina Hernández – Jefe OTI