ANEXO No. 01

1 OBJETO CONTRACTUAL

Contratar la renovación de licencias, soporte especializado, mantenimiento, administración, capacitación y transferencia de conocimiento de la plataforma LUMU Defender para la Sociedad de Activos Especiales SAE S.A.S., orientada a la detección, análisis, **contención** y respuesta de compromisos de ciberseguridad mediante el monitoreo continuo de metadatos de red, inteligencia de amenazas e integración con las herramientas de seguridad institucionales, bajo modalidad Software como Servicio (SaaS).

2 GENERALIDADES DEL PROCESO

La Sociedad de Activos Especiales SAE S.A.S. requiere mantener y fortalecer las capacidades de visibilidad y detección temprana de amenazas cibernéticas mediante la continuidad de la plataforma LUMU Defender, actualmente implementada en la Entidad. La solución permite identificar compromisos de seguridad en tiempo real mediante el análisis de metadatos de red y la correlación con múltiples fuentes de inteligencia de amenazas.

El servicio debe permitir la detección, análisis y gestión de eventos relacionados con:

1) Malware.
2) Phishing.
3) Comando y Control (C2).
4) Minería maliciosa.
5) Spam.
6) Amenazas avanzadas persistentes.
7) Comunicaciones maliciosas.
8) Indicadores de compromiso (IoC).

La solución debe proporcionar visibilidad sobre ambientes:

1) On-Premise.
2) Nube pública.
3) Infraestructuras híbridas.
4) Usuarios remotos.

3 REQUERIMIENTOS TÉCNICOS

3.1 Requisitos generales

El proveedor reconoce que la solución ofertada debe cubrir, como mínimo, las siguientes capacidades:

3.1.1 La solución está basada en modalidad SaaS

1) La solución debe estar en la capacidad de procesar datos sin importar el formato enviado
2) La solución debe tener la capacidad de recolectar, procesar y analizar "mínimo" las consultas de:
   a) DNS de la organización
   b) Netflows
   c) Logs de Proxy y/o Firewall
   d) Spambox
   e) VPN

3.1.2 La recolección debe como "mínimo":

a) Mantenerse implementada mediante utilización ilimitada de ambientes virtuales o instancias en nube sin la necesidad de hardware de propósito específico, El OFERENTE debe dejar de manera clara los prerrequisitos y cantidades para la arquitectura apropiada en el CLIENTE.
b) Estar basada en metadata, no debe incluir los paquetes de datos.
c) Recolectar, procesar y analizar metadatos de dispositivos remotos con o sin agente para Windows Linux y MacOS.

3.1.3 El proceso de análisis de la metadata de la organización debe estar basado como "mínimo"en:

a) Correlación contra más de 60 fuentes de ciberinteligencia
b) Analizadores supervisados de machine learning e inteligencia artificial
c) Algoritmos no supervisados de machine learning e inteligencia artificial
d) Comportamiento de la red sin previo aprendizaje identificando amenazas desde el primer día de instalación sin casos de uso.
e) La solución debe proporcionar contexto de cada compromiso con referencias internas y externas para entender la naturaleza de este

3.1.4 Comportamiento y respuesta

a) Ante la detección de un compromiso, la solución debe responder de forma automática con la infraestructura de defensa "mínimo" perímetro para ajustar las políticas de bloqueo pertinentes.
b) La solución debe clasificar el análisis del compromiso de manera automática en:
c) Malware, Comando & Control, Rasomware, Phishing, Spam, Mining.
d) La solución debe realizar una revisión histórica de nuevos ataques para identificar compromiso histórico basado en nueva información.
e) La solución debe entregar los IoCs por cada compromiso detectado y se debe poder descargar directamente de la



plataforma.

f) La solución debe tener certificación que garantice que no se captura información confidencial del cliente.
g) La solución debe incluir el análisis de cada incidente y vista global de técnicas y tácticas con base en la matriz MITRE ATT&CK
h) La solución debe estar listada en reportes de los siguientes analistas: Gartner, Forrester, ESG y EMA.
i) La solución debe contar con almacenamiento y retención de eventos y/o logs hasta por dos (2) años.
j) La solución debe contar con colectores de eventos predefinidos, que integren a los principales fabricantes del mercado como Cisco, Paloalto, Fortinet, entre otros
k) La solución debe tener la capacidad de adicionar nuevas fuentes de ciberinteligencia con conceptos tales como BYOTI "Bring your own threat intelligence"
l) La solución debe tener una vista de incidentes que permita gestionar incidentes abiertos, en trabajo, cerrados o silenciados llevando registro de las acciones tomadas en los mismos.
m) La solución debe poder integrarse con otras herramientas de seguridad para detección y respuesta ante amenazas como un EDR o XDR, firewall, SIEM.

3.1.5 NO se aceptarán soluciones tipo:

o Firewalls
o SIEM
o Sandboxing
o EDR

3.1.6 Debe mantenerse el producto ya implementado (LUMU Defender)

3.1.7 El proveedor declara conocer y aceptar que:

1) La reasignación de créditos durante la vigencia contractual no genera pérdida de licencias, módulos o capacidades previamente contratadas.
2) El modelo permite adaptarse a variaciones del inventario sin modificaciones contractuales adicionales, siempre que se mantenga la equivalencia funcional.

3) Las licencias actualmente implementadas en la Entidad presentan vencimiento a partir del 15 de agosto de 2026; sin embargo, la información histórica, configuraciones e integraciones asociadas a la plataforma permanecen disponibles y forman parte del activo tecnológico que se busca preservar mediante la presente contratación.

4) La estimación de consumo para la SAE bajo el modelo por licencias es:
1250 Licencias para 12 meses

3.2 Arquitectura General

La solución debe operar en modalidad SaaS administrada por el fabricante.
La plataforma debe estar en capacidad de:

1) Procesar información independientemente de su formato.
2) Analizar metadatos sin almacenar el contenido completo del tráfico.
3) Realizar análisis en tiempo real.
4) Integrarse con la infraestructura actual de seguridad de la SAE.

3.3 Fuentes de Información Mínimas

La solución debe recolectar, procesar y analizar como mínimo:

1) Consultas DNS.
2) NetFlow.
3) Logs de Firewall.
4) Logs de Proxy.
5) VPN.
6) Spambox.
7) Dispositivos remotos.

3.4 Capacidad de Recolección

La solución debe:

1) Utilizar entornos virtuales o instancias cloud.
2) No requerir hardware especializado.
3) Recolectar exclusivamente metadatos.
4) Soportar agentes para Windows.
5) Soportar agentes para Linux.
6) Soportar agentes para macOS.
7) Soportar análisis sin agente cuando sea aplicable.

3.5 Motor de Análisis e Inteligencia

La solución debe incorporar:

1) Correlación contra más de 60 fuentes de inteligencia de amenazas.
2) Machine Learning supervisado.
3) Machine Learning no supervisado.
4) Modelos de Inteligencia Artificial.
5) Detección sin aprendizaje previo.



6) Identificación de amenazas desde el primer día de implementación.

3.6 Análisis de Compromisos

La plataforma debe:

1) Identificar compromisos históricos.
2) Ejecutar búsqueda retrospectiva de amenazas.
3) Entregar contexto detallado de cada incidente.
4) Generar indicadores de compromiso (IoC).
5) Permitir exportar los IoC para análisis externo.
6) Presentar referencias internas y externas sobre cada amenaza detectada.

3.7 Clasificación de Amenazas

La solución debe clasificar automáticamente los compromisos detectados en categorías como:

1) Malware.
2) Command & Control.
3) Ransomware.
4) Phishing.
5) Spam.
6) Minería maliciosa.

3.8 Integración con Framework MITRE ATT&CK

La solución debe:

1) Incorporar análisis basado en MITRE ATT&CK.
2) Mostrar tácticas observadas.
3) Mostrar técnicas detectadas.
4) Presentar análisis contextual de incidentes.

3.9 Gestión de Incidentes

La solución debe permitir:

1) Apertura de incidentes.
2) Gestión de incidentes en proceso.
3) Cierre de incidentes.
4) Silenciamiento controlado.
5) Registro de actividades realizadas.
6) Trazabilidad completa de acciones.

3.10 Integraciones de Seguridad

1) La plataforma debe integrarse con:
2) Firewalls.



3) EDR.
4) XDR.
5) SIEM.
6) Plataformas de inteligencia de amenazas.
7) Soluciones de monitoreo existentes.

3.11 Retención de Información

La solución debe mantener:

1) Almacenamiento de eventos.
2) Retención histórica de hasta dos (2) años.
3) Acceso a registros históricos para investigaciones forenses.

3.12 REQUERIMIENTOS OPERATIVOS

La plataforma debe contar con:

1) Consola web centralizada.
2) Acceso seguro.
3) Gestión basada en roles.
4) Visibilidad en tiempo real.
5) Dashboards ejecutivos y técnicos.
6) Capacidades de exportación de reportes.

4 Requerimientos de Privacidad y Tratamiento de Datos Personales

El proveedor debe garantizar que toda la operación, procesamiento, almacenamiento y transmisión de datos derivados del uso de la plataforma de ciberseguridad cumpla con la Ley 1581 de 2012, el Decreto 1377 de 2013, el régimen de protección de datos personales en Colombia, así como los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de Gobierno Digital establecidos por el MinTIC.

En consecuencia, el proveedor debe:

a. Asegurar la protección de datos personales, incluyendo información sensible, telemetría, registros de seguridad, política de acceso y cualquier dato procesado por la plataforma.
b. Garantizar el cifrado en tránsito y en reposo de toda la información, de acuerdo con estándares internacionales (TLS 1.2 o superior).
c. Declarar expresamente la ubicación geográfica de los datos, indicando país y normativa de protección aplicable.
d. Asegurar que no realizará transferencias internacionales de datos sin la autorización previa, expresa y escrita de la SAE S.A.S.

Las copias impresas de este documento no son controladas.
Si hace copia impresa verifique su actualización en el portal de intranet SAE SAS.

e. Garantizar mecanismos seguros de eliminación, anonimización y reversibilidad al finalizar el contrato.
f. Asegurar que los datos procesados no serán utilizados para fines distintos al cumplimiento del objeto contractual.
g. Mantener registros de auditoría sobre acceso, modificación, consulta, eliminación y uso de los datos.
h. Garantizar que cualquier subcontratista cumpla los mismos estándares de privacidad y protección de datos.
i. El proveedor será responsable por cualquier incumplimiento, fuga, alteración, pérdida o acceso no autorizado a datos personales o datos institucionales como consecuencia de mala práctica, omisión o fallas en los controles de seguridad.

5 ADMINISTRACIÓN

La plataforma debe operar en modalidad SaaS y proporcionar mecanismos de administración centralizada que garanticen control, trazabilidad, seguridad y eficiencia en la operación.

Como mínimo, debe cumplir con las siguientes características:

5.1 Administración y acceso a consolas

1) Consolas 100% web, provistas directamente por el fabricante.
2) Autenticación robusta mediante MFA (mínimo dos factores).
3) Gestión de accesos basada en roles y perfiles, con permisos granulares para administración, operación, auditoría y monitoreo.
4) Integración con Active Directory y/o Azure Active Directory, permitiendo:
   a) Autenticación unificada (SSO)
   b) Control de accesos centralizado
   c) Trazabilidad completa sobre actividades administrativas
5) Registro detallado de logs de administración y auditoría, incluyendo creación de políticas, cambios, accesos, acciones de respuesta y eventos relevantes.

5.2 Operación y co-administración

El proveedor debe realizar co-administración de la plataforma junto con el equipo de TI y Seguridad de la SAE, garantizando gestión continua y acompañamiento experto.

5.2.1 Se requiere la entrega de capacitación técnica a los funcionarios designados por SAE, incluyendo:

1) Operación general de la plataforma

2) Gestión de políticas
3) Revisión de alertas y dashboard
4) Buenas prácticas de administración

5.2.2 Las políticas de seguridad deben gestionarse de manera centralizada para:

1) Endpoints
2) Correos y colaboración Microsoft 365
3) Seguridad web
4) Servidores y workloads

6 Integraciones

La plataforma debe contar con capacidades de integración nativa que permitan interoperabilidad con soluciones existentes en SAE:

a. SIEM / SOAR

1) Integración mediante estándares:
    - Syslog
    - CEF
    - LEEF
    - SNMP

2) Exposición de APIs para consulta de alertas, eventos, telemetría, inventario y acciones de respuesta.

b. Integraciones con nube

1) Conectores cloud para:
    - Amazon Web Services (AWS)
    - Microsoft Azure
    - Google Cloud Platform (GCP)

c. Integración con servicios de identidad

Las copias impresas de este documento no son controladas.
Si hace copia impresa verifique su actualización en el portal de intranet SAE SAS.

7 REQUERIMIENTOS DEL PROVEEDOR

El proveedor debe acreditar certificaciones técnicas vigentes tanto del fabricante como del personal asignado, así como su condición de partner autorizado para la comercialización, soporte y administración de la plataforma ofertada. Estas certificaciones serán requisito habilitante para la evaluación técnica de la oferta.

1) El proveedor debe acreditar:
a) Distribución autorizada por fabricante.
b) Certificaciones técnicas vigentes.
c) Experiencia en proyectos similares.
d) Personal certificado en LUMU Defender.

1) Así mismo debe demostrar:
a) Entre uno (1) y cinco (5) contratos ejecutados o en ejecución similares al objeto contractual.
b) Certificaciones de experiencia emitidas por los contratantes.
c) Membresía Gold, Platinum o equivalente frente al fabricante.

8 ACUERDOS A NIVEL DE SERVICIO (ANS)

Los siguientes Acuerdos de Nivel de Servicio (ANS) son de obligatorio cumplimiento por parte del contratista durante toda la vigencia del contrato. Su incumplimiento dará lugar a la aplicación de penalidades, retenciones, y/o demás medidas previstas en el contrato y en la normatividad aplicable.

8.1 Disponibilidad del servicio

1) Disponibilidad del servicio SaaS

El contratista garantizará una disponibilidad mínima del 99,99% mensual para:

a) DNS Forwarders: 99,99%
b) Portal de gestión: 99,99%

2) Cómputo de disponibilidad

Se considera indisponibilidad cualquier evento que impida total o parcialmente el acceso normal a:
a) Consola SaaS

Las copias impresas de este documento no son controladas.
Si hace copia impresa verifique su actualización en el portal de intranet SAE SAS.



b) Funciones de administración
c) Integraciones con SIEM/SOAR o conectores cloud

3) El cálculo de disponibilidad será:

$$Disponibilidad = 1 - \left[\frac{Minutos\ de\ indisponibilidad\ atribuibles\ al\ contratista}{Mínutos\ totales\ del\ mes}\right]$$

4) No se excluirán del cálculo las interrupciones por mantenimiento, salvo:

a) Mantenimientos programados notificados con mínimo 72 horas de antelación, y
b) Interrupciones que no excedan 4 horas mensuales, y que se realicen entre las 00:00 y 04:00 horas (zona horaria local).

5) Evidencias

El contratista debe suministrar, a requerimiento y sin costo, evidencias técnicas de disponibilidad, incluyendo:

a) Registros de monitoreo
b) Métricas de uptime
c) Logs del proveedor
d) Reportes automáticos de la plataforma

9 Gestión de incidentes y soporte técnico

El contratista debe garantizar atención en los siguientes tiempos máximos, contados desde la apertura del ticket:

Nivel de alerta	Tiempo máximo de respuesta	Tiempo máximo de solución/mitigación	Horario
Crítica	≤ 1 hora	≤ 4 horas	7x24
Alta	≤ 2 horas	≤ 8 horas	5x8
Media	≤ 4 horas	≤ 24 horas	5x8
Baja	≤ 24 horas	≤ 72 horas	5x8

Las copias impresas de este documento no son controladas.
Si hace copia impresa verifique su actualización en el portal de intranet SAE SAS.

Nota: Si existe un incidente crítico que continúe afectando disponibilidad o protección de activos, se activa automáticamente un proceso de escalamiento, incluyendo soporte de ingeniería especializada (L2/L3) por parte del fabricante, sin costo adicional.

10 Informes y reportes obligatorios

El contratista debe entregar dentro de los primeros cinco (5) días hábiles de cada mes un informe que contenga como mínimo:

1) Estado general del servicio.
2) Disponibilidad.
3) Incidentes detectados.
4) Hallazgos relevantes.
5) Amenazas identificadas.
6) Estado de compromisos.
7) Actividades de soporte realizadas.
8) Recomendaciones de mejora.

El informe debe ser aprobado por la supervisión del contrato; su no entrega será causal de aplicación de penalidad.

11 Penalidades por incumplimiento

Las penalidades se aplicarán mensualmente sobre el valor facturado del periodo respectivo, según la siguiente tabla:

Tipo de incumplimiento	Penalidad
Incumplimiento en ANS de criticidad baja	**0,5%**
Incumplimiento en ANS de criticidad media	**1,0%**
Incumplimiento en ANS de criticidad alta	**1,5%**
Indisponibilidad mensual inferior a 99,99%	**1% adicional**
No entrega del informe mensual	**0,5% por cada día de retraso**, hasta 5%

Aspecto clave agregado: Si en un mismo mes se presentan dos o más incumplimientos, las penalidades serán acumulativas.

12 Servicio continuo, monitoreo y acompañamiento

El proveedor debe garantizar:

1) Actualizaciones de la plataforma.
2) Actualización de inteligencia de amenazas.
3) Corrección de errores.
4) Ajustes de configuración.
5) Optimización continua del servicio.

13 MANTENIMIENTO

Garantizar el mantenimiento preventivo, correctivo y evolutivo de toda la plataforma de ciberseguridad, asegurando su operación continua, segura y actualizada durante la totalidad de la vigencia del contrato. Las actividades de mantenimiento deben incluir, como mínimo, las siguientes obligaciones:

13.1 Mantenimiento preventivo obligatorio

Realizar mantenimiento preventivo orientado a garantizar la estabilidad y actualización de la plataforma, que incluye:

13.2 Actualizaciones de componentes

Aplicación oportuna de:

1) Actualizaciones de la plataforma.
2) Actualización de inteligencia de amenazas.
3) Corrección de errores.
4) Ajustes de configuración.
5) Optimización continua del servicio.
6) Conectores (SIEM/SOAR)
7) Agentes de endpoint y workload

Todas las actualizaciones deben realizarse sin afectar continuidad del servicio, salvo aquellas que requieran ventana programada.

13.3 Ventanas de mantenimiento programado



Las actividades que impliquen interrupciones deben notificarse a la Sociedad de Activos Especiales SAE SAS con 72 horas de antelación como mínimo, justificación técnica, impacto estimado, plan de reversión. La ventana no podrá superar 4 horas mensuales.

13.4 Pruebas y validaciones

1) Validar la correcta aplicación de actualizaciones.
2) Reportar cualquier impacto detectado.
3) Garantizar reversión en caso de afectaciones.

13.5 Mantenimiento correctivo obligatorio

Corregir cualquier falla o comportamiento anómalo de la plataforma, incluyendo:

13.5.1 Corrección de errores como:

1) Incidentes funcionales
2) Fallos en agentes
3) Fallas de comunicación con la consola
4) Anomalías en telemetría
5) Errores de políticas
6) Incompatibilidades o fallas derivadas de actualizaciones

La corrección debe cumplir los ANS de tiempos de respuesta y solución.

13.5.2 Acceso obligatorio a soporte especializado L2/L3

El contratista debe gestionar y asegurar el acceso a ingeniería especializada del fabricante (niveles L2 y L3), sin costos adicionales , el cual es obligatorio cuando el incidente esté relacionado con fallos internos del software o del backend SaaS.

14 Protección de datos y cumplimiento normativo

El contratista garantizará que toda la operación se realice conforme a estándares de seguridad de la información:

14.1 Controles obligatorios

1) Cifrado de comunicaciones (TLS 1.2 o superior).
2) Controles de acceso basados en roles.
3) Registros detallados de auditoría.
4) Detección y reporte de accesos irregulares.

14.2 Plantillas DLP y cumplimiento

Los módulos correspondientes deben incluir plantillas y políticas compatibles con marcos de cumplimiento como:

1) PCI-DSS
2) HIPAA
3) GDPR
4) ISO 27001
5) Buenas prácticas de seguridad en entornos Microsoft 365 y cloud

El contratista debe apoyar en la configuración inicial de estas plantillas.

15 Comunicaciones y canales de soporte

15.1 El contratista debe proporcionar los siguientes canales de soporte:

1) Mesa de ayuda
2) Correo electrónico
3) Línea telefónica directa
4) Portal de soporte / panel técnico de la consola

15.2 Disponibilidad de soporte

1) Incidentes críticos: 7x24
2) Incidentes no críticos: 5x8

15.3 Notificaciones automáticas



La plataforma debe generar alertas automáticas por:

1) Detecciones críticas
2) Cuarentenas
3) Violaciones de políticas
4) Parches virtuales aplicados
5) Alertas de postura en la nube
6) Cambios relevantes en políticas
7) Notificaciones deben enviarse al correo de los administradores designados por SAE.

16 GARANTÍA COMERCIAL Y DE CALIDAD

El servicio objeto del contrato se presta bajo modalidad Software como Servicio (SaaS), razón por la cual la garantía comercial no se configura como una garantía tradicional sobre bienes físicos, sino como un compromiso integral del proveedor respecto a la calidad, continuidad, actualización y soporte del servicio, en los términos establecidos en el contrato y en los Acuerdos de Nivel de Servicio (ANS).

El proveedor debe garantizar, como mínimo, los siguientes aspectos:

16.1 Garantía de continuidad y disponibilidad del servicio

Operación continua de la plataforma SaaS conforme a la disponibilidad mínima establecida en los ANS (99,99% mensual). Entrega de evidencias técnicas de monitoreo, uptime, registros de fallas y mantenimiento cuando sean solicitadas por la SAE.

16.2 Garantía de calidad del servicio - El proveedor garantiza que el servicio:

1) Cumple con los niveles de servicio definidos en la ficha técnica y el contrato.
2) Funciona conforme a la arquitectura definida por el fabricante.
3) Es operado bajo estándares de seguridad, buenas prácticas de la industria y políticas de calidad del fabricante.
4) Incluye mecanismos automáticos de detección, protección, corrección y monitoreo continuo.

16.3 Garantía de actualizaciones y mantenimiento - El proveedor debe asegurar la actualización constante y oportuna de:

1) Actualizaciones de la plataforma.

2) Actualización de inteligencia de amenazas.
3) Corrección de errores.
4) Ajustes de configuración.
5) Optimización continua del servicio.

Todas las actualizaciones deben ejecutarse sin afectar la continuidad del servicio, o mediante ventanas programadas previamente notificadas a la SAE.

16.4 Garantía de soporte técnico especializado - El proveedor garantiza:

1) Soporte técnico en español.
2) Atención prioritaria según criticidad del incidente (7x24 para críticos).
3) Escalamiento automático de incidentes que afecten la protección, disponibilidad o integridad de la plataforma.

16.5 Garantía de cumplimiento de los ANS - El proveedor garantiza el cumplimiento de:

1) Tiempos de respuesta.
2) Tiempos de solución.
3) Entrega de reportes mensuales.
4) Disponibilidad del servicio.
5) Mantenimiento preventivo y correctivo.
6) Operación segura y trazable.

El incumplimiento de los ANS activará las penalidades contractuales respaldadas en la sección correspondiente.

16.6 Garantía de seguridad y confidencialidad - El proveedor debe garantizar:

1) Cifrado de comunicaciones.
2) Controles de acceso basados en roles.
3) Protección de datos y cumplimiento normativo (DLP, PCI-DSS, GDPR, etc.).
4) Registros completos de auditoría accesibles para la SAE.
5) Procesamiento seguro de información y telemetría.

El proveedor será responsable por cualquier falla derivada de mala práctica, omisión o actualización incorrecta.

16.7 Verificación de cumplimiento - El cumplimiento de la garantía se verificará mediante:

Las copias impresas de este documento no son controladas.
Si hace copia impresa verifique su actualización en el portal de intranet SAE SAS.



1) Informes mensuales obligatorios.
2) Registros de disponibilidad.
3) Evidencias de soporte e incidentes.
4) Métricas de calidad del servicio.
5) Auditorías o revisiones solicitadas por la SAE.

17 FASES DE LA EJECUCIÓN CONTRACTUAL

La ejecución del contrato se desarrollará en tres fases: Inicio, Desarrollo y Cierre, cada una con entregables verificables por parte de la Sociedad de Activos Especiales SAE SAS y obligaciones específicas del contratista. El cumplimiento de estas fases debe evidenciarse documentalmente y será requisito para la continuidad del contrato y/o trámite de pagos.

17.1 Fase de Inicio

Corresponde al periodo entre la firma del acta de inicio y la puesta en operación formal del servicio.
El contratista debe cumplir, como mínimo, con los siguientes entregables:

17.1.1 Actividades administrativas

1) Presentación, aprobación y radicación de garantías contractuales.
2) Designación formal del equipo técnico y de soporte del contratista.
3) Definición de canales y procedimientos de comunicación y escalamiento.

17.1.2 Activación del servicio

1) Activación total de las licencias y módulos contratados.
2) Habilitación de las consolas SaaS de administración.
3) Configuración inicial de acceso seguro (MFA, roles, permisos, perfiles).

17.1.3 Configuración base de la plataforma

Configuración inicial mínima para dejar operativa la solución en los siguientes dominios:



1) Endpoints: instalación de agentes, políticas de protección base, telemetría.
2) Correo Microsoft 365: políticas de protección, sandboxing, time-of-click.
3) Web Security: reglas iniciales, filtrado base, inspección HTTPS.
4) Servidores/Workloads: IPS, virtual patching, monitoreo de integridad.
5) Cloud Security: conexión con AWS, Azure o GCP según aplique.

17.1.4 Capacitación de arranque

Inducción operativa para el equipo técnico designado por la SAE.
Capacitación en:

1) Administración general
2) Políticas
3) Monitoreo de alertas
4) Detección y respuesta
5) Manejo de reportes

17.1.5 Entregables de la fase

1) Acta de inicio firmada.
2) Documento de roles y accesos configurados.
3) Certificación de activación de licencias.
4) Documento de configuración inicial.
5) Plan de trabajo y cronograma de operación.
6) Evidencia de capacitaciones.

17.2 Fase de Desarrollo

Corresponde al periodo activo del contrato e incluye la prestación continua del servicio, soporte, mantenimiento y mejora continua.

El contratista debe cumplir con los siguientes requisitos:

17.2.1 Operación continua del servicio

Funcionamiento permanente del servicio conforme a los ANS establecidos.
Gestión centralizada de la plataforma en modalidad SaaS.

Las copias impresas de este documento no son controladas.
Si hace copia impresa verifique su actualización en el portal de intranet SAE SAS.

17.2.2 Administración y co-administración

Acompañamiento permanente en la administración del servicio.
Configuración, ajuste y optimización de:

1) Políticas de endpoint
2) Políticas de correo
3) Políticas web
4) Políticas de servidores/workloads

17.2.3 Mantenimiento preventivo y correctivo

1) Actualizaciones de parches, firmas y motores.
2) Aplicación de actualizaciones del backend SaaS.
3) Gestión de virtual patching/IPS y vulnerabilidades.
4) Corrección de incidentes conforme a los ANS.
5) Escalamiento automático a soporte especializado L2/L3.

17.2.4 Actividades de plataforma SaaS

1) Hunting proactivo de amenazas.
2) Análisis de telemetría multicapas.
3) Correlación avanzada de eventos.
4) Recomendaciones de mejora continua de postura de seguridad.

17.2.5 Reportes y seguimiento

1) Entrega mensual de informes obligatorios dentro de los primeros 5 días hábiles.
2) Indicadores de disponibilidad, incidentes, vulnerabilidades y actividades.
3) Reuniones mensuales de seguimiento técnico y operativo.

17.2.6 Entregables de la fase

1) Reportes mensuales.
2) Evidencias de mantenimiento.

Las copias impresas de este documento no son controladas.
Si hace copia impresa verifique su actualización en el portal de intranet SAE SAS.



3) Logs de soporte y atención de incidentes.
4) Ajustes de configuración y políticas.
5) Actas de seguimiento mensual (si la SAE las requiere).

17.3 Fase de Cierre del Contrato

Corresponde a la etapa final para validar cumplimiento y garantizar la correcta terminación del servicio.

17.4 Verificación de obligaciones

El contratista debe garantizar:

1) Cumplimiento total de obligaciones contractuales, técnicas y ANS.
2) Entrega de todos los reportes pendientes.
3) Cierre de tickets abiertos o plan documentado de transición.

17.5 Informe final

Entrega obligatoria de:

1) Consolidado de incidentes.
2) Disponibilidad acumulada.
3) Actividades de mantenimiento.
4) Estado de licencias y capacidades utilizadas.
5) Estado de postura de seguridad.
6) Recomendaciones finales para la SAE.

17.6 Transición o renovación

Si aplica renovación:

1) Revisión de capacidades y licencias utilizadas.
2) Proyección de necesidades
3) Soporte para migración de configuración existente

17.7 3.4 Acta de terminación

Firma del acta de terminación del contrato.



Validación del supervisor sobre la conformidad de todos los entregables.

Dado que el servicio se presta en modalidad Software como Servicio (SaaS), no se exigirá personal mínimo como requisito técnico obligatorio, por cuanto la calidad y continuidad del servicio dependen de la plataforma contratada y de los compromisos operativos establecidos en los Acuerdos de Nivel de Servicio (ANS).

No obstante, el contratista debe garantizar, durante toda la vigencia del contrato, la disponibilidad del equipo humano necesario y suficiente para asegurar la correcta prestación del servicio, incluyendo actividades de operación, administración, soporte especializado, mantenimiento y capacitación.

18 Personal técnico del contratista

La SAE puede solicitar aclaraciones sobre perfiles, experiencia, certificaciones o funciones del personal del contratista.
Requerir el reemplazo de personal que afecte la calidad del servicio o incumpla obligaciones, sin generar costos adicionales.
Exigir evidencia de acceso del contratista al soporte oficial del fabricante (L2/L3).

Estas solicitudes se enmarcan en los principios de planeación, eficiencia, responsabilidad, transparencia y selección objetiva.

18.1 Equipo técnico del contratista

El contratista deberá garantizar durante toda la vigencia contractual la disponibilidad del recurso humano, capacidades técnicas y mecanismos de soporte necesarios para el cumplimiento integral del objeto contratado. La Entidad no exige un equipo mínimo habilitante ni un número determinado de profesionales para participar en el proceso; sin embargo, el contratista deberá asegurar la disponibilidad de personal idóneo y del soporte especializado del fabricante para atender las actividades requeridas durante la ejecución contractual.
Para efectos de la correcta prestación del servicio, el contratista deberá garantizar la cobertura de las siguientes funciones operativas y técnicas:

18.1.1 Administración y operación de la plataforma

Configuración de políticas.
Supervisión de agentes y colectores.
Actividades de co-administración con la SAE.

18.1.2 Soporte técnico

Atención y solución de incidentes en los tiempos establecidos en los ANS.
Soporte en español en modalidad 7x24/5x8 según criticidad.
Gestión de escalamiento a niveles L2 y L3 del fabricante.

18.1.3 Ingeniería especializada (directa o fabricante)

Diagnóstico avanzado.
Remediación de fallas complejas.
Ajustes privados, hotfixes y soporte de backend SaaS.

18.1.4 Capacitación

Transferencia de conocimiento al equipo de la SAE.
Actualizaciones periódicas cuando se modifiquen módulos, políticas o funcionalidades del servicio.

18.2 Obligaciones del contratista respecto al personal

El contratista debe garantizar:

1) Disponibilidad permanente del personal requerido para cumplir con los ANS.
2) Reemplazo inmediato de personal en caso de ausencia, sin afectar la operación.
3) Que todo el personal asignado cuente con conocimientos y experiencia en plataformas de seguridad.
4) Acceso a personal certificado por el fabricante cuando la naturaleza del incidente lo requiera.
5) Atención oportuna de requerimientos del supervisor o interventor de la SAE.

19 LUGAR DE EJECUCIÓN

El servicio se ejecutará en todas las sedes de la Sociedad de Activos Especiales – SAE S.A.S., incluyendo instalaciones administrativas, regionales, operativas, centros de datos, oficinas remotas, puntos de acceso y cualquier otra ubicación donde la Entidad cuente con infraestructura tecnológica, usuarios autorizados o activos informáticos que requieran cobertura de la plataforma de ciberseguridad.

Debido a que el servicio se presta en modalidad Software como Servicio (SaaS), la ejecución incluye también:

Los ambientes tecnológicos de los usuarios y equipos conectados a la red institucional, sin importar su ubicación geográfica.
Los servidores, cargas de trabajo y servicios alojados en entornos de nube pública o híbrida utilizados por la SAE.
Los endpoints, equipos móviles, estaciones de trabajo, servidores y recursos de TI ubicados física o remotamente.

Las copias impresas de este documento no son controladas.
Si hace copia impresa verifique su actualización en el portal de intranet SAE SAS.



El contratista debe garantizar la correcta prestación del servicio en todas las sedes actuales y en aquellas adicionales que la SAE llegare a habilitar durante la vigencia, sin costos adicionales, siempre que dichas sedes hagan parte de la operación institucional.

20 INFORMES Y/O REPORTES

El contratista debe entregar los informes y reportes derivados de la operación de la plataforma, necesarios para el seguimiento técnico, funcional y operativo del servicio. Los informes deben ser claros, verificables, completos y suministrados en los formatos solicitados por la SAE.

20.1 Informe mensual de servicio (obligatorio)

El contratista debe entregar a la Oficina de Tecnologías de la Información (OTI) un informe mensual dentro de los primeros cinco (5) días hábiles de cada mes, que incluya como mínimo:

20.1.1 Integridad del servicio

Disponibilidad mensual del servicio SaaS y de la consola de gestión y resumen de eventos que hayan afectado la continuidad.

1) Incidentes y soporte
2) Incidentes atendidos clasificados por criticidad, cumplimiento de los tiempos de respuesta y solución conforme a los ANS, y acciones aplicadas en incidentes críticos o de alto impacto.

20.1.2 Detecciones y protección

1) Métricas de detección de:
2) Malware
3) Phishing
4) BEC (Business Email Compromise)
5) Acciones automáticas o manuales aplicadas (cuarentenas, bloqueos, aislamientos).

20.1.3 Actividades en plataforma

1) Tendencias de amenazas observadas en el periodo.
2) Actividades de threat hunting, correlación y análisis.
3) Casos relevantes con su línea de tiempo (timeline) y análisis de causa raíz (RCA) cuando aplique.



20.2 Reportes ad-hoc o técnicos especializados

La plataforma debe permitir y el contratista debe entregar reportes técnicos a requerimiento de la SAE, con disponibilidad inmediata o en tiempos razonables según su complejidad.
Estos reportes podrán incluir, entre otros:

20.2.1 Seguridad endpoint / antimalware

Eventos de detección, cuarentena o bloqueo.
Análisis de comportamiento o actividad sospechosa.

20.2.2 Reputación y análisis web

URL, dominios y archivos bloqueados por reputación.
Resultados de inspección HTTP/HTTPS.

20.3 Formatos y entrega

El contratista debe garantizar que todos los reportes:

Puedan exportarse en PDF, XLSX y DOCX.
Puedan descargarse desde la consola o ser entregados por el proveedor.
Se entreguen dentro de los plazos indicados por la SAE cuando sean solicitados.
Incluyan evidencias técnicas cuando la SAE lo requiera (logs, capturas, verificaciones, etc.).

Al presentar su oferta o cotización, el proveedor declara formalmente que conoce, acepta y cumple de manera integral con los requerimientos técnicos establecidos en la presente Ficha Técnica y en los Términos de Referencia aplicables, sin limitaciones, exclusiones o condicionamientos.

ARZUZA PEREZ ERVIN LUIS

Firmado digitalmente por ARZUZA PEREZ ERVIN LUIS
Fecha: 2026.11.04 16:20:16 -05'00'

Aprobó: Ing. Ervin Luis Arzuza Pérez
Revisó: Ing. Juan Carlos Alarcon Suescum
Proyectó: Ing. Jeysson Zamudio

*Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma del / la ordenadora (a) del gasto de la SAE SAS.

