ANEXO No. 01 – FICHA TÉCNICA Y ESPECIFICACIONES TÉCNICAS MÍNIMAS

1 OBJETO CONTRACTUAL

Contratar la renovación y adquisición de licencias, así como la prestación de los servicios asociados a una plataforma integral de seguridad para detección y respuesta extendida (XDR), que incluya protección de endpoints, servidores y cargas de trabajo, seguridad de correo y colaboración en Microsoft 365, prevención de pérdida de datos (DLP), control de aplicaciones, seguridad web, gestión de postura de seguridad en nube, gestión de exposición al riesgo cibernético, soporte técnico especializado, mantenimiento, actualizaciones, administración centralizada y operación bajo modalidad Software como Servicio (SaaS), para la Sociedad de Activos Especiales S.A.S.

2 REQUISITOS TÉCNICOS

La Sociedad de Activos Especiales SAE SAS requiere la operación de una plataforma integral de ciberseguridad, bajo modalidad Software como Servicio (SaaS), que permita fortalecer la protección, monitoreo, detección, respuesta y gestión del riesgo tecnológico en toda la infraestructura institucional.

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.

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

Las capacidades descritas en el presente capítulo corresponden a requisitos generales mínimos de obligatorio cumplimiento. Los componentes funcionales y especificaciones técnicas detalladas desarrolladas posteriormente en el capítulo “COMPONENTES FUNCIONALES” complementan, amplían y precisan dichas capacidades, por lo que ambos conjuntos de requisitos son acumulativos y deberán ser cumplidos integralmente por la solución ofertada.

2.1 Endpoint Protection

La solución debe incluir capacidades de gestión de:

a) Antimalware y protección contra ransomware con mecanismos de rollback.
b) Control de aplicaciones y dispositivos.
c) Prevención de pérdida de datos (DLP).
d) Firewall de host y capacidades de aislamiento.
e) Consola de administración SaaS con telemetría en tiempo real.

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

2.2 Seguridad Web

La solución debe incluir capacidades de gestión de:

a) Inspección completa de tráfico HTTP/HTTPS.
b) Sandbox para análisis avanzado de amenazas web.

2.3 Protección de correo y colaboración Microsoft 365

La solución debe incluir capacidades de gestión de:

a) Sandboxing de adjuntos y URLs.
b) Protección time-of-click.
c) Detección y mitigación de ataques BEC.
d) DLP para correo.
e) Gestión de cuarentenas.
f) Latencia promedio de procesamiento de correo inferior a un (1) minuto en condiciones normales de operación.

2.4 Plataforma XDR multi-dominio

La solución debe incluir capacidades de gestión de:

a) Threat hunting con soporte para IoC, YARA, STIX y TAXII.
b) Correlación multicapas (endpoint, servidor, correo, web, nube).
c) Timelines de incidentes y análisis de causa raíz (RCA).
d) Acciones de respuesta en contexto.
e) Integración SIEM mediante Syslog/CEF/LEEF/SNMP y APIs.
f) Conector nativo para Splunk.

2.5 Workload Security

La solución debe incluir capacidades de gestión de:

a) IPS y virtual patching.
b) Monitoreo de integridad de archivos (FIM).
c) Escaneo de vulnerabilidades.
d) Firewall para workloads.
e) Inspección de logs y actividad sospechosa.
f) Cobertura para máquinas virtuales, contenedores y autoscaling.
g) Conectores cloud operativos para los entornos de nube pública utilizados por la Sociedad de Activos Especiales S.A.S. (SAE S.A.S.), incluyendo AWS, Microsoft Azure y/o Google Cloud Platform (GCP), según aplique a la infraestructura tecnológica institucional durante la ejecución contractual.

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

2.6 Cloud Risk Management

La solución debe incluir capacidades de gestión de:

a) Monitoreo continuo multi-nube.
b) Evaluación de configuración frente a estándares y buenas prácticas.
c) Alertas y remediación automática (cuando aplique).
d) Reportes calendarizados de postura cloud.
e) API pública para integración con herramientas de la SAE.

2.7 Aceptación del modelo de asignación por créditos (2026)

El proveedor declara conocer y aceptar que:

a) El modelo de consumo por créditos vigente desde 2026 no modifica el alcance técnico, las capacidades ni la calidad del servicio ofertado.
b) La reasignación de créditos durante la vigencia contractual no genera pérdida de licencias, módulos o capacidades previamente contratadas.
c) El modelo permite adaptarse a variaciones del inventario sin modificaciones contractuales adicionales, siempre que se mantenga la equivalencia funcional.

d) La SAE S.A.S. cuenta actualmente con una solución de seguridad implementada para la protección de endpoints, servidores, cargas de trabajo, correo electrónico y demás activos tecnológicos institucionales.

e) Las licencias asociadas a dicha solución alcanzaron su fecha de vencimiento durante la vigencia 2026, razón por la cual la presente contratación busca garantizar la renovación y continuidad de las capacidades de seguridad actualmente utilizadas por la Entidad.

f) Mientras se culmina el presente proceso contractual, la Oficina de Tecnología y Sistemas de la Información realiza seguimiento permanente a los riesgos asociados a la continuidad de los controles de seguridad digital institucional, con el propósito de mitigar los impactos derivados de la expiración del licenciamiento.

g) La vigencia del nuevo licenciamiento se contará a partir de la activación efectiva de las licencias suministradas como resultado del presente proceso contractual y no tendrá efectos retroactivos respecto de licencias o suscripciones previamente vencidas.

h) La estimación de consumo para la SAE S.A.S. bajo el modelo de licenciamiento por créditos corresponde a:

- 283.000 créditos para una vigencia de doce (12) meses.
  La estimación anterior fue calculada con base en el inventario tecnológico institucional proyectado para la vigencia contractual, incluyendo estaciones de trabajo, servidores, cargas de trabajo, servicios de correo electrónico, componentes de seguridad cloud y demás activos tecnológicos protegidos por la solución.

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

La cantidad de créditos requerida contempla la cobertura de la infraestructura tecnológica actualmente utilizada por la Entidad y las variaciones razonables asociadas a la operación institucional durante la vigencia contractual.

En caso de que la Entidad requiera consumos superiores a los estimados inicialmente, cualquier ampliación de capacidades o adquisición adicional de créditos deberá sujetarse a los mecanismos contractuales y presupuestales aplicables, sin que ello implique obligación automática para la Entidad ni modificación unilateral del valor contratado.

La solución deberá incorporar, como mínimo, los siguientes componentes funcionales:

2.8 COMPONENTES FUNCIONALES

2.8.1 Protección de endpoints

La solución deberá permitir:

1) Aislamiento remoto de dispositivos comprometidos.
2) Recuperación automática de archivos mediante rollback ante eventos de ransomware.
3) Protección contra amenazas fileless y ataques basados en PowerShell.
4) Protección mediante análisis de comportamiento, Machine Learning y reputación de archivos.
5) Despliegue de agentes mediante instalación remota, scripts, correo electrónico o paquetes de instalación.
6) Protección de agentes contra desinstalación no autorizada.
7) Administración de equipos tanto dentro como fuera de la red corporativa.

2.8.2 Seguridad web

La solución deberá incluir:

1) Categorización dinámica de URLs en tiempo real.
2) Reputación de sitios web y reputación de archivos descargados.
3) Inspección HTTPS mediante análisis de tráfico cifrado.
4) Protección para usuarios conectados fuera de la red institucional.
5) Sandbox para análisis de archivos y objetos sospechosos.

2.8.3 Seguridad de correo y colaboración para Microsoft 365

La solución deberá incluir:

1) Filtrado avanzado de amenazas en correo y plataformas de colaboración.
2) Protección para OneDrive y SharePoint Online.
3) Protección para servicios de almacenamiento en nube como Google Drive, Dropbox y Box.

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

4) Protección Time-of-Click para enlaces contenidos en correos electrónicos.
5) Detección de ataques de phishing, spear phishing y Business Email Compromise (BEC).
6) Machine Learning para análisis de mensajes y archivos sospechosos.
7) Gestión centralizada de cuarentenas.
8) Latencia promedio de procesamiento inferior a un (1) minuto.

2.8.4 Plataforma de Detección y Respuesta Extendida (XDR)

Debe permitir correlación multicapas, análisis avanzado, visibilidad consolidada, investigación automatizada, priorización de alertas y capacidades de respuesta integral a incidentes.

La plataforma XDR deberá incluir:

1) Threat Hunting proactivo.
2) Soporte para indicadores de compromiso (IoC).
3) Integración con reglas YARA.
4) Integración mediante estándares STIX y TAXII.
5) Capacidades de Root Cause Analysis (RCA).
6) Visualización gráfica del ciclo completo de ataque.
7) Correlación de eventos entre Endpoint, correo, web, servidores, identidad y nube.
8) Integración con framework MITRE ATT&CK.
9) Respuesta contextualizada desde una consola unificada.

2.8.5 Seguridad de Identidades

La plataforma deberá integrarse con Active Directory, Microsoft Entra ID, Okta u otros servicios de identidad compatibles con LDAP –

La solución debe permitir:

1) Detectar compromisos de cuentas.
2) Correlacionar eventos de identidad con telemetría XDR.
3) Identificar usuarios de alto riesgo.
4) Aplicar acciones correctivas como bloqueo de cuentas, cierre de sesiones o restablecimiento de credenciales.

2.8.6 Protección de servidores y cargas de trabajo (workloads)

La solución deberá incluir:

1) Protección para entornos físicos, virtuales, nube y contenedores.
2) Protección para cargas de trabajo basadas en Docker.
3) Escaneo continuo de vulnerabilidades.
4) Protección mediante IPS y Virtual Patching.
5) Firewall bidireccional administrado centralmente.
6) Monitoreo de integridad de archivos (FIM).
7) Inspección y correlación de logs.

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

8) Recomendación automática de reglas de protección según vulnerabilidades detectadas.

2.8.7 Gestión de postura de seguridad en la nube

La solución debe contar con cobertura sobre AWS, Azure y/o GCP, conforme a los entornos cloud utilizados por la SAE S.A.S., con monitoreo continuo, identificación de configuraciones inseguras, alertamiento, recomendaciones de remediación y cumplimiento de buenas prácticas.

2.9 CUMPLIMIENTO NORMATIVO Y LINEAMIENTOS NACIONALES

La solución objeto de contratación deberá ser plenamente compatible con los lineamientos, políticas y marcos normativos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, incluyendo la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), los lineamientos de servicios en la nube para entidades públicas, las disposiciones de interoperabilidad, gestión de riesgos y continuidad del negocio, así como con la normativa nacional vigente en materia de protección de datos personales, ciberseguridad y gestión tecnológica. En consecuencia, el proveedor deberá garantizar que la plataforma cumpla con las buenas prácticas y estándares aplicables, asegurando su adecuada alineación con los requisitos técnicos, regulatorios y de gobernanza digital que rigen a la SAE S.A.S.

2.10 GESTIÓN DE EXPOSICIÓN Y RIESGO CIBERNÉTICO

La solución deberá proporcionar capacidades de gestión continua de exposición y riesgo cibernético que permitan:

a) Identificar activos expuestos a Internet.
b) Correlacionar vulnerabilidades, configuraciones inseguras e identidades.
c) Priorizar riesgos según criticidad y exposición.
d) Visualizar mapas de riesgo corporativo.
e) Identificar vectores potenciales de ataque.
f) Generar recomendaciones de remediación.
g) Incorporar capacidades de inteligencia artificial para análisis y priorización de riesgos.

3 REQUERIMIENTOS OPERATIVOS

La plataforma debe proveer consolas de administración 100% web, perfiles basados en roles y controles de acceso granulares, reportes bajo demanda y reportes calendarizados e integraciones nativas con SIEM/SOAR, utilizando estándares como Syslog, CEF, LEEF, STIX/TAXII y APIs.

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

3.1 MODELO DE LICENCIAMIENTO

A partir de 2026, el fabricante adoptó un esquema de consumo por créditos, el cual:

Mantiene un costo consolidado por la suite completa.
Permite redistribuir capacidades según cambios en el inventario o necesidades operativas durante la vigencia.
Evita la pérdida de licencias o módulos adquiridos previamente.

Como parte de la evolución tecnológica de la solución actualmente implementada en la SAE S.A.S. y del modelo de licenciamiento por créditos adoptado por el fabricante, se presenta la siguiente equivalencia de denominaciones comerciales con el único propósito de facilitar la identificación de los componentes que hacen parte de la renovación tecnológica requerida por la Entidad:

a) Vision One ASRM → Cyber Risk Exposure Management – Essentials.

b) Smart Protection Complete se desagregó en:
   1) Endpoint Security Essentials
   2) Email & Collaboration Security – Core
   3) XDR for Email (EmDR)

c) Cloud One – Workload Security with XDR → Endpoint Security Pro.

d) Cloud One – Conformity → Cloud Risk Management (2001–2500 assets).

Las referencias anteriormente relacionadas no constituyen requisitos funcionales adicionales ni incrementan el alcance técnico exigido por la Entidad. Su inclusión tiene carácter exclusivamente informativo y obedece a la necesidad de identificar la correspondencia entre las denominaciones comerciales utilizadas en la solución actualmente implementada y la estructura de licenciamiento vigente del fabricante.

3.2 ADMINISTRACIÓN

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

Como mínimo, deberá cumplir con las siguientes características:

3.2.1 Administración y acceso a consolas

1) Consolas 100% web, provistas directamente por el fabricante.
2) Autenticación robusta mediante MFA (mínimo dos factores).

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

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.

3.2.2 Operación y co-administración

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

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

a) Operación general de la plataforma
b) Gestión de políticas
c) Revisión de alertas y dashboard
d) Buenas prácticas de administración

Las políticas de seguridad deberán gestionarse de manera centralizada para:

1) Endpoints
2) Correos y colaboración Microsoft 365
3) Seguridad web
4) Servidores y workloads
5) Postura de seguridad en la nube

3.2.3 Integraciones

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

1) SIEM / SOAR
   a) Integración mediante estándares:
      i) Syslog
      ii) CEF
      iii) LEEF
      iv) SNMP

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

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

c) Conector nativo para Splunk (on-premise o cloud).

2) Integraciones con nube

a) Conectores cloud para:
   i) Amazon Web Services (AWS)
   ii) Microsoft Azure
   iii) Google Cloud Platform (GCP)

3) Capacidad de ingestión, correlación y análisis dentro del motor XDR multi-dominio, integrando telemetría de endpoint, correo, web, servidores y nube.

4) Integración con servicios de identidad

La solución deberá integrarse con plataformas de gestión de identidad y acceso tales como Active Directory, Microsoft Entra ID (Azure AD), LDAP, SAML u otras equivalentes, permitiendo autenticación centralizada, control de acceso adaptativo y correlación de eventos de identidad dentro de la plataforma XDR.

3.2.4 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, compensaciones por nivel de servicio, y/o demás medidas previstas en el contrato y en la normatividad aplicable.

3.2.4.1 Disponibilidad del servicio

1) Disponibilidad del servicio SaaS

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

i) Consola de administración SaaS.
ii) Plataforma de análisis XDR.
iii) Módulos de protección de endpoints, correo, web, servidores y nube.
iv) APIs e integraciones.

Parágrafo: La disponibilidad exigida deberá corresponder como mínimo a los niveles de servicio oficialmente garantizados por el fabricante de la solución ofertada para los componentes SaaS incluidos en la contratación. Para efectos de la medición del

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

ANS, se entenderán como eventos atribuibles al contratista aquellos relacionados con la gestión, configuración, soporte, operación, administración o integración de la solución bajo su responsabilidad, así como aquellos eventos cuya gestión requiera escalamiento o intervención del fabricante a través de los canales de soporte contratados.

2) Cómputo de disponibilidad

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

i) Consola SaaS
ii) Funciones de administración
iii) Motor de correlación XDR
iv) Recepción, procesamiento o envío de telemetría
v) APIs
vi) Integraciones con SIEM/SOAR o conectores cloud

3) Computo de disponibilidad:

Para efectos de la medición del ANS, se entenderán como eventos de indisponibilidad atribuibles al contratista aquellos relacionados con:

- Fallas en actividades de administración, operación o soporte bajo su responsabilidad.
- Errores de configuración aplicados por el contratista.
- Interrupciones derivadas de procedimientos de mantenimiento ejecutados sin autorización o por fuera de las ventanas aprobadas.
- Incumplimientos en los procesos de actualización, monitoreo o gestión operativa de la solución.
- Fallas del servicio SaaS atribuibles al fabricante, cuando el contratista no gestione oportunamente el respectivo escalamiento, seguimiento o acompañamiento requerido para su atención.

No se considerarán atribuibles al contratista los eventos derivados de:

- Fallas de infraestructura tecnológica propia de la SAE S.A.S.
- Problemas de conectividad externa de terceros ajenos al servicio.
- Casos de fuerza mayor o caso fortuito debidamente demostrados.
- Ventanas de mantenimiento autorizadas conforme a lo establecido en la presente ficha técnica.

La disponibilidad mensual se calculará mediante la siguiente fórmula:

Disponibilidad (%) = [(Minutos totales del mes − Minutos de indisponibilidad atribuibles al contratista) / Minutos totales del mes] × 100

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

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

Mantenimientos programados notificados con mínimo 72 horas de antelación, y 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 deberá suministrar, a requerimiento y sin costo, evidencias técnicas de disponibilidad, incluyendo:

i) Registros de monitoreo
ii) Métricas de uptime
iii) Logs del proveedor
iv) Reportes automáticos de la plataforma

3.2.5 Gestión de incidentes y soporte técnico

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

Criterios para el cómputo de los tiempos de atención

Los tiempos de respuesta y solución establecidos en la presente ficha técnica se contabilizarán a partir de la apertura formal del ticket a través de los canales de soporte definidos por el contratista.

Para los incidentes clasificados como Alta, Media y Baja, los tiempos se contabilizarán en horas hábiles dentro del esquema de atención 5x8, entendido como de lunes a viernes, en días hábiles, entre las 8:00 a.m. y las 5:00 p.m., hora legal colombiana, excluyendo sábados, domingos y festivos.

Para los incidentes clasificados como Críticos, los tiempos se contabilizarán de manera continua bajo esquema 7x24, incluyendo fines de semana y días festivos.
La clasificación inicial de la criticidad del incidente será realizada por la SAE S.A.S. al momento de registrar el ticket. En caso de que el contratista considere que la clasificación no corresponde al impacto real del evento reportado, podrá solicitar su reclasificación mediante justificación técnica escrita. Mientras dicha solicitud es evaluada, prevalecerá la clasificación inicialmente definida por la SAE S.A.S. para efectos del cómputo de los ANS.

Tabla 1 Tiempos de respuesta y solución de tickets

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

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

Baja	≤ 24 horas	≤ 72 horas	5x8

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.

3.2.6 Informes y reportes obligatorios

El contratista deberá entregar, dentro de los primeros cinco (5) días hábiles de cada mes, un informe mensual integral de ejecución del servicio, dirigido al supervisor del contrato y/o al apoyo a la supervisión designado por la Entidad.

El informe constituirá el soporte para la verificación de cumplimiento contractual y para el trámite de los pagos correspondientes a los servicios de coadministración y soporte técnico especializado, y deberá contener como mínimo la siguiente información:

1. Nivel real de disponibilidad de la solución (con evidencias).
2. Incidentes abiertos, cerrados y en proceso de tratamiento.
3. Cumplimiento de tiempos de respuesta y solución de acuerdo con los tiempos máximos de respuesta descritos en la tabla “Tiempos de respuesta y solución de tickets”.
4. Tendencias de amenazas.
5. Detecciones correlacionadas del XDR.
6. Situación de vulnerabilidades detectadas.
7. Eventos críticos y su resolución.
8. Cambios aplicados en políticas y configuraciones.
9. Cumplimiento del plan de capacidades (créditos).
10. Recomendaciones de mejora continua y hallazgos operativos.

Adicionalmente, el informe deberá incluir:

- Actividades de coadministración ejecutadas durante el período.
- Tickets atendidos y gestionados.
- Casos escalados al fabricante.
- Cumplimiento de ANS.
- Actividades de soporte técnico especializado niveles 1, 2 y 3.
- Evidencias documentales que permitan verificar la correcta ejecución de los servicios contratados.

El informe deberá ser aprobado por la supervisión del contrato designado por la SAE S.A.S; su no entrega será causal de aplicación de penalidad.

3.2.7 Penalidades por incumplimiento

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

El incumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos en la presente ficha técnica dará lugar a la aplicación de descuentos por nivel de servicio, sin perjuicio de los demás mecanismos contractuales previstos en el contrato.

La aplicación de dichos descuentos deberá observar el procedimiento previsto en el contrato, el Manual de Compras y Adquisiciones (MN-GC-001) vigente y las garantías de contradicción del contratista.:

Tipo de incumplimiento	Descuento máximo
Incumplimiento en ANS de criticidad crítica	**2,0%**
Incumplimiento en ANS de criticidad alta	**1,5%**
Incumplimiento en ANS de criticidad media	**1,0%**
Incumplimiento en ANS de criticidad baja	**0,5%**
Disponibilidad mensual inferior al ANS exigido	**1,0% adicional**
No entrega del informe mensual	**0,5% por día de retraso hasta un máximo de 5%**

Parágrafo 1. Los descuentos por ANS serán calculados sobre el valor mensual correspondiente a los servicios de soporte técnico especializado y coadministración del período afectado.

Parágrafo 2. La suma de los descuentos aplicables en un mismo período no podrá superar el diez por ciento (10%) del valor mensual de los servicios asociados al ANS.

Parágrafo 3. Los descuentos por nivel de servicio tendrán naturaleza de mecanismo de compensación asociado al incumplimiento de ANS y deberán desarrollarse en detalle dentro de la minuta contractual, incluyendo procedimiento, soportes, oportunidad de contradicción y forma de compensación económica.

Regla de acumulación de descuentos por ANS

Los descuentos asociados al incumplimiento de los ANS podrán ser acumulativos cuando en un mismo período de evaluación se presenten dos (2) o más incumplimientos independientes.

3.2.8 Servicio continuo, monitoreo y acompañamiento

El contratista deberá garantizar:

1) Monitoreo 7x24 del funcionamiento de la plataforma.
2) Seguimiento continuo de alertas críticas y altas.
3) Acompañamiento experto en incidentes calificados como críticos y altos.
4) Acceso a soporte de fabricante (L2/L3) sin costos adicionales.

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

4 REQUERIMIENTOS DE CUMPLIMIENTO Y CERTIFICACIONES DEL PROVEEDOR Y DEL FABRICANTE.

El proveedor deberá acreditar el cumplimiento de los requisitos relacionados con certificaciones del fabricante, condición de canal autorizado y certificaciones técnicas del personal mínimo exigido, de conformidad con los requisitos habilitantes definidos en el Estudio Previo y en el Documento de Condiciones Generales y Reglas del Proceso de Contratación.

En particular, el proponente deberá acreditar:

a) La condición de fabricante, distribuidor autorizado, partner, reseller, integrador o figura equivalente reconocida por el fabricante de la solución ofertada, en los términos establecidos en los requisitos técnicos habilitantes.
b) La vigencia de las certificaciones exigidas para los perfiles técnicos mínimos requeridos por la Entidad.
c) La capacidad para comercializar, implementar, activar, administrar y escalar la solución ante el fabricante durante la ejecución contractual.

La documentación aportada será objeto de verificación durante la etapa de evaluación de ofertas y deberá cumplir las condiciones establecidas en los documentos del proceso.

5 REQUERIMIENTOS DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES

El proveedor deberá 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 deberá:

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, centro de datos, proveedor de infraestructura utilizado, finalidad del tratamiento y normativa de protección de datos aplicable.
d. Informar previamente a la SAE S.A.S. cuando la operación de la solución implique transmisión o tratamiento internacional de datos personales, garantizando el cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013 y las demás disposiciones aplicables en materia de protección de datos personales.
   Cuando se requieran transferencias internacionales de datos personales en los términos de la normativa colombiana, el contratista deberá informar previamente a la SAE S.A.S. y dar cumplimiento a los mecanismos legales, contractuales y de autorización que resulten aplicables para su ejecución.
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.

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

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.

La evaluación de la ubicación declarada de los datos y de los mecanismos de tratamiento utilizados por la solución se realizará durante la etapa de implementación del servicio, con base en los criterios de seguridad de la información, gestión del riesgo, protección de datos personales y lineamientos institucionales establecidos por la SAE S.A.S.

6 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 deberán incluir, como mínimo, las siguientes obligaciones:

6.1 Mantenimiento preventivo obligatorio

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

6.1.1 Actualizaciones de componentes

Aplicación oportuna de:

1) Parches de seguridad
2) Actualizaciones de firmas
3) Motores antimalware
4) Módulos XDR
5) Componentes de nube
6) Conectores (SIEM/SOAR)
7) Agentes de endpoint y workload

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

6.1.2 Ventanas de mantenimiento programado

Las actividades que impliquen interrupciones deberán 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.

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

6.1.3 Pruebas y validaciones

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

6.2 Mantenimiento correctivo obligatorio

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

6.2.1 Corrección de errores

La corrección deberá cumplir los ANS de tiempos de respuesta y solución, incluyendo:

a) Incidentes funcionales
b) Fallos en agentes
c) Fallas de comunicación con la consola
d) Anomalías en telemetría
e) Errores de políticas
f) Incompatibilidades o fallas derivadas de actualizaciones

6.2.2 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.

Obligatorio cuando el incidente esté relacionado con fallos internos del software o del backend SaaS.

6.3 Virtual Patching, IPS y gestión de vulnerabilidades. El contratista deberá garantizar:

6.3.1 Virtual patching / IPS

a) Aplicación de reglas de protección (IPS) que mitiguen vulnerabilidades conocidas y cero-día.
b) Generación automática o asistida de firmas para ataques detectados.
c) Implementación sin afectar operación de servidores o aplicaciones críticas.

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

6.3.2 Gestión de vulnerabilidades - Identificación continua de vulnerabilidades en:

a) Endpoints
b) Servidores
c) Workloads cloud
d) Aplicaciones expuestas

6.3.3 Clasificación de riesgo (CVSS). Reporte mensual de:

a) Vulnerabilidades detectadas
b) Reglas IPS aplicadas
c) Vulnerabilidades mitigadas
d) Vulnerabilidades pendientes con recomendaciones

6.4 Protección de datos y cumplimiento normativo

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

6.4.1 Controles obligatorios

a) Cifrado de comunicaciones (TLS 1.2 o superior).
b) Controles de acceso basados en roles.
c) Registros detallados de auditoría.
d) Detección y reporte de accesos irregulares.

6.4.2 Plantillas DLP y cumplimiento

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

a) PCI-DSS
b) Ley 1581 de 2012 y sus decretos reglamentarios
c) ISO 27001
d) Buenas prácticas de seguridad en entornos Microsoft 365 y cloud

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

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

6.5 Comunicaciones y canales de soporte

El contratista deberá proporcionar los siguientes canales de soporte:

a) Mesa de ayuda
b) Correo electrónico
c) Línea telefónica directa
d) Portal de soporte / panel técnico de la consola

6.5.1 Disponibilidad de soporte

a) Incidentes críticos: 7x24
b) Incidentes no críticos: 5x8

6.5.2 Notificaciones automáticas

La plataforma deberá generar alertas automáticas por:

a) Detecciones críticas
b) Cuarentenas
c) Violaciones de políticas
d) Parches virtuales aplicados
e) Alertas de postura en la nube
f) Cambios relevantes en políticas
g) Notificaciones deberán enviarse al correo de los administradores designados por SAE.

7 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 deberá garantizar, como mínimo, los siguientes aspectos:

7.1 Garantía de continuidad y disponibilidad del servicio

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

Operación continua de la plataforma SaaS conforme a la disponibilidad mínima establecida en los ANS (99,99% mensual).
La disponibilidad incluye todos los módulos del servicio: protección de endpoints, correo, web, servidores, nube, XDR, APIs e integraciones.
Entrega de evidencias técnicas de monitoreo, uptime, registros de fallas y mantenimiento cuando sean solicitadas por la SAE.

7.2 Garantía de calidad del servicio

El proveedor garantiza que el servicio:

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

7.3 Garantía de actualizaciones y mantenimiento

El proveedor debe asegurar la actualización constante y oportuna de:

a) Parches de seguridad.
b) Firmas antimalware.
c) Motores y componentes XDR.
d) Conectores cloud y SIEM/SOAR.
e) Módulos y versiones SaaS.

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

7.4 Garantía de soporte técnico especializado

El proveedor debe garantizar:

a) Soporte técnico en español.
b) Atención prioritaria según criticidad del incidente (7x24 para críticos).
c) Acceso a soporte especializado de ingeniería L2 y L3 del fabricante sin costo adicional.
d) Escalamiento automático de incidentes que afecten la protección, disponibilidad o integridad de la plataforma.

7.5 Garantía de cumplimiento de los ANS

El proveedor debe garantizar el cumplimiento de:

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

a) Tiempos de respuesta.
b) Tiempos de solución.
c) Entrega de reportes mensuales.
d) Disponibilidad del servicio.
e) Mantenimiento preventivo y correctivo.
f) Operación segura y trazable.

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

7.6 Garantía de seguridad y confidencialidad

El proveedor debe garantizar:

a) Cifrado de comunicaciones.
b) Controles de acceso basados en roles.
c) Protección de datos y cumplimiento normativo (DLP, PCI-DSS, GDPR, etc.).
d) Registros completos de auditoría accesibles para la SAE.
e) Procesamiento seguro de información y telemetría.

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

7.7 Verificación de cumplimiento

El cumplimiento de la garantía se verificará mediante:

a) Informes mensuales obligatorios.
b) Registros de disponibilidad.
c) Evidencias de soporte e incidentes.
d) Métricas de calidad del servicio.
e) Auditorías o revisiones solicitadas por la SAE.

8 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.

8.1 Fase de Inicio

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

Corresponde al período comprendido entre la suscripción del acta de inicio y la puesta en operación formal de la solución. Esta fase tendrá una duración máxima de cinco (5) días hábiles contados a partir de la suscripción del acta de inicio, plazo dentro del cual el contratista deberá realizar la activación integral de las licencias, la habilitación de las consolas de administración, la configuración base de la solución y la ejecución de las actividades iniciales requeridas para su operación.

El contratista deberá cumplir, como mínimo, con los siguientes entregables:

8.1.1 Actividades administrativas

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

8.1.2 Activación del servicio

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

La activación efectiva de las licencias deberá quedar completada dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de inicio. La vigencia del licenciamiento se contará a partir de la fecha de activación certificada por el fabricante o distribuidor autorizado y, en todo caso, deberá cubrir la totalidad del plazo contractual.
Los Acuerdos de Nivel de Servicio (ANS) serán exigibles a partir de la puesta en operación formal de la solución y de la activación efectiva de las licencias, una vez culminadas las actividades previstas para la fase de inicio.

8.1.3 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 los servicios de nube pública utilizados por la SAE S.A.S. (AWS, Azure y/o GCP), según aplique.

8.1.4 Inducción operativa y transferencia de conocimiento para el equipo técnico designado por la SAE S.A.S

La capacitación deberá realizarse durante la fase de inicio del contrato y antes de la puesta en operación formal de la solución.

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

Como mínimo deberá cumplir las siguientes condiciones:

- Intensidad mínima: ocho (8) horas.
- Modalidad: presencial, virtual o mixta.
- Participantes: mínimo cinco (5) funcionarios o colaboradores designados por la SAE S.A.S.
- Material de apoyo digital suministrado por el contratista.
- Espacio para preguntas y ejercicios prácticos sobre la plataforma.
- Registro de asistencia y evidencia documental de ejecución.

Como evidencia de cumplimiento, el contratista deberá entregar al supervisor del contrato:

- Listado de asistentes.
- Registro o control de asistencia.
- Material utilizado durante la capacitación.
- Memoria o presentación de los temas desarrollados.
- Acta o constancia de realización de la actividad.

8.1.5 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.

8.2 Fase de Desarrollo

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

El contratista deberá cumplir con los siguientes requisitos:

8.2.1 Operación continua del servicio

1) Funcionamiento permanente del servicio conforme a los ANS establecidos.
2) 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.

8.2.2 Administración y co-administración

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

   a) Políticas de endpoint
   b) Políticas de correo
   c) Políticas web
   d) Políticas de servidores/workloads
   e) Postura de seguridad cloud

8.2.3 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.

8.2.4 Actividades XDR

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

8.2.5 Reportes y seguimiento

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

8.2.6 Entregables de la fase

1) Reportes mensuales.
2) Evidencias de mantenimiento.
3) Logs de soporte y atención de incidentes.
4) Ajustes de configuración y políticas.

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

5) Actas de seguimiento mensual (si la SAE las requiere).

8.3 Fase de Cierre del Contrato

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

8.3.1 Verificación de obligaciones

El contratista deberá 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.

8.3.2 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.

8.3.3 Transición o renovación

Si aplica renovación:

1) Revisión de capacidades y créditos consumidos
2) Proyección de necesidades
3) Soporte para migración de configuración existente

8.3.4 Acta de terminación

1) Firma del acta de terminación del contrato.
2) Validación del supervisor sobre la conformidad de todos los entregables.

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

8.4 Recursos de personal

Aunque la solución opera bajo modalidad Software como Servicio (SaaS), la ejecución contractual comprende servicios especializados de soporte técnico niveles L1, L2 y L3, coadministración, acompañamiento técnico, gestión de incidentes, atención de requerimientos, escalamiento al fabricante y transferencia de conocimiento. En consecuencia, la SAE S.A.S. exigirá el equipo técnico mínimo definido en el Estudio Previo y en el Documento de Condiciones Generales y Reglas del Proceso de Contratación, el cual deberá mantenerse disponible durante toda la ejecución contractual para garantizar el cumplimiento de los ANS y la adecuada prestación de los servicios asociados a la solución contratada.

Los siguientes requerimientos se enmarcan en los principios de planeación, eficiencia, responsabilidad, transparencia y selección objetiva.

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

8.4.1 El contratista deberá 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 XDR, seguridad endpoint, seguridad cloud y correo.
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.

8.4.2 Equipo técnico del contratista

El contratista deberá disponer de un equipo técnico que permita cumplir integralmente con el alcance del contrato, compuesto por perfiles que cubran, como mínimo, las siguientes funciones:

8.4.3 Administración y operación de la plataforma

Funciones

1. Configuración de políticas.
2. Supervisión de agentes y conectores.
3. Actividades de co-administración con la SAE.

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

8.5 Soporte técnico

Funciones

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

8.6 Ingeniería especializada (directa o fabricante)

Funciones

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

8.7 Capacitación

Funciones

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

9 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.

El contratista deberá 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.

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

10 INFORMES Y/O REPORTES

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

10.1 Informe mensual de servicio (obligatorio)

El contratista deberá entregar al supervisor del contrato y/o al apoyo a la supervisión designado por la SAE S.A.S., dentro de los primeros cinco (5) días hábiles de cada mes, un informe mensual integral de ejecución del servicio que incluya como mínimo:

1. Integridad del servicio

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

2. Incidentes y soporte

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.

3. Detecciones y protección

Métricas de detección de:

a) Malware
b) Phishing
c) BEC (Business Email Compromise)
d) Acciones automática o manuales (cuarentenas, bloqueos, asilamientos)

4. Actividades XDR

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

5. Vulnerabilidades y postura cloud

a) Vulnerabilidades identificadas y su criticidad.
b) Reglas IPS/virtual patching aplicadas.
c) Hallazgos de postura de seguridad cloud (AWS, Azure, GCP).
d) Recomendaciones y acciones de mejora continua.

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

10.2 Reportes ad-hoc o técnicos especializados

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

1. Seguridad endpoint / antimalware

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

2. Integridad y protección avanzada

a) FIM (monitoreo de integridad de archivos).
b) IPS / virtual patching aplicado.
c) Bloqueos del firewall de host y reglas aplicadas.

3. Reputación y análisis web

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

4. Correo y colaboración

a) Actividad del sandbox.
b) Eventos de time-of-click.
c) Bloqueos por reputación o heurísticos.
d) Casos de BEC detectados o mitigados.

5. XDR

a) Lineas de tiempo (timeline) de incidentes relevantes.
b) RCA (Root Cause Analysis) de investigaciones solicitadas.
c) Correlación entre dominios (endpoint, correo, servidor, nube).

6. Cumplimiento y DLP

a) Eventos relacionados con plantillas de cumplimiento (PCI-DSS, GDPR, etc.).
b) Activaciones de políticas DLP.

7. Nube (cloud)

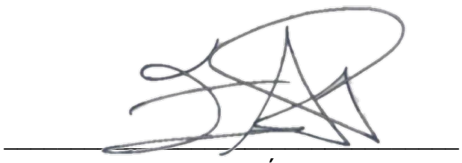
Las copias impresas de este documento no son controladas.
Si hace copia impresa verifique su actualización en el portal de intranet SAE SAS.

a) Alertas de postura de seguridad.
b) Configuraciones peligrosas detectadas.
c) Reportes de exposición o riesgo.

10.3 Formatos y entrega

El contratista deberá garantizar que todos los reportes:

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



ERVIN LUIS ARZUZA PÉREZ
Jefe de la Oficina de Tecnologías y Sistemas de la Información

Aprobó: Ing. Ervin Luis Arzuza Pérez - Jefe OTI
Revisó: Ing. Juan Carlos Alarcon Suescún - Lider Seguridad OTI
Proyectó: Ing. Jeysson Steven Zamudio Bonilla

*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.

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