ANEXO

FICHA TÉCNICA

OBJETO: ***10-0-7-26*** - ***FORTALECER EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI PARA LA AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA A TRAVÉS DE LAS HERRAMIENTAS ESPECIALIZADAS (LICENCIAMIENTO DE SOFTWARE Y SOPORTE) DE MONITOREO FORTISIEM DE MONITOREO DE RED SOLARWINDS, DE MESA DE AYUDA ARANDA; ASI COMO LA CONTRATACIÓN DE SERVICIOS ESPECIALIZADOS DE UN CENTRO DE OPERACIÓN DE SEGURIDAD (SOC).***

Con base en el clasificador de bienes y servicios de las Naciones Unidas, a continuación, se establece el sector económico al que pertenecen los bienes y servicios a contratar:

CÓDIGO	SEGMENTO	FAMILIA	CLASE
43233200	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección
43222500	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red
43232800	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de administración de redes
43233700	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de administración de sistemas
81111800	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios Informáticos	Servicios de sistemas y administración de componentes de sistemas
81111811	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas

Para dar cumplimiento al objeto, el contratista deberá tener en cuenta las especificaciones de los servicios a adquirir por parte de la **AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES - ANLA** establecidas en las siguientes especificaciones técnicas, aclarando que no se aceptaran propuestas parciales:

DESCRIPCIÓN DE LOS BIENES Y SERVICIOS A ADQUIRIR

1. LICENCIAMIENTO DE SOFTWARE PARA LA HERRAMIENTA ESPECIALIZADA DE MONITOREO FORTISIEM

Ítem	Licencias	Descripción	Cantidad
1	FC6Z-15-FSM99-240-02-00: Premium Forticare License Support Contract (1 - 500 points) for FortiSIEM hardware appliance. 1 device or 2 End points or 3 Windows Agents equals 1 point.	Este licenciamiento es requerido por la entidad debido a que permite la actualización de parches del software, cuando se presenta un mal funcionamiento o una falla en alguno de los componentes del equipo por un año (del 17 de nov 2026 al 18 de nov 2027).	1
2	FC6Z-15-FSM98-149-02-00: (1 - 500 Points) FortiSIEM Indicators of Compromise (IOC) Service	Indicadores de Compromiso (IoC) para El appliance FSM-2000F: FSM2KFT318000053 de FortiSiem por un año (del 17 de nov 2026 al 18 de nov 2027).	1

2. CARACTERISTICAS DEL SERVICIO ESPECIALIZADO DE UN CENTRO DE OPERACIÓN DE SEGURIDAD (SOC).

La Entidad requiere adquirir el **servicio SOC** a través del cual el contratista garantice el monitoreo, alertamiento y gestión de los incidentes de los eventos de seguridad detectados por el correlacionador **FORTISIEM**, servicio a prestar desde la fecha definida en el cronograma establecido por las partes y hasta el **31 de diciembre de 2026.** El servicio debe contar con las siguientes características:

2.1 DESCRIPCIÓN GENERAL DE LOS SERVICIOS

- Monitoreo y análisis de eventos e incidentes de ciberseguridad.
- Monitorear la deepweb, darkweb y reputación de la ANLA frente a amenazas cibernéticas
- Gestión de alertas, eventos e incidentes de seguridad de la información y ciberseguridad.
- Analizar las posibles fallas que se puedan presentar en las plataformas, las cuales puedan generar un impacto negativo sobre los servicios.
- Documentar los incidentes de seguridad con su respectiva solución, para ir alimentando una base del conocimiento.
- Generación de casos de uso de acuerdo con el modelo de operación de la entidad.
- Afinamiento y propuestas de casos de uso en el correlacionador de eventos alineados con las necesidades de la ANLA.
- Realizar integraciones de tipo Security Fabric con plataformas Solarwinds, Fortinet, Checkpoint y F5.

- Activar un Takedown (identificar y eliminar contenido malicioso o fraudulento en línea) por demanda de la ANLA.
- Seguimiento Mensual de la operación del servicio a través de un informe.

Este servicio también debe incluir el desarrollo de las fases de levantamiento de información, análisis, pruebas, transferencia de conocimiento para mínimo 3 funcionarios de la Oficina de tecnologías de la información de la ANLA, estabilización, soporte, mantenimiento y operación de los servicios de Ciberseguridad y red requeridos por la Entidad.

2.2 GENERALIDADES

El CONTRATISTA deberá proveer un servicio integral de seguridad gestionada que incluya todos los recursos que requiera para proveer los servicios requeridos por la Entidad, bajo condiciones de calidad, capacidad, oportunidad y seguridad.

El CONTRATISTA deberá contar con un servicio de SOC 'Security Operation Center' con disponibilidad 7X24. (7 días, 24 horas,), que se encuentre certificado en ISO 27001.

El CONTRATISTA deberá proveer un servicio integral de seguridad gestionada que incluya todos los recursos que requiera para proveer los servicios requeridos por la ENTIDAD, bajo condiciones de calidad, capacidad, oportunidad y seguridad.

El CONTRATISTA deberá contar con un servicio de SOC 'Security Operation Center' con disponibilidad 7X24. (7 días, 24 horas,), que se encuentre certificado en ISO 27001 y sea miembro activo en FIRST.

El CONTRATISTA deberá tener un SOC propio ubicado en la ciudad de Bogotá, el cual será validado por la Entidad garantizando que cumple todos los lineamientos y controles de seguridad de la información.

El CONTRATISTA debe tener políticas de seguridad física para el acceso al SOC (centros de datos y sala de monitoreo), las cuales deben ser presentadas a la Entidad, con el fin de reducir el riesgo debido a amenazas o peligros del entorno como accesos no autorizados.

El proveedor deberá tener los roles y responsabilidades del grupo de operaciones del SOC, claramente definido, en lo que respecta al monitoreo, correlación, análisis y de tendencias de seguridad y atención de requerimientos, manejo y contención de incidentes de seguridad, inteligencia de la amenaza y Hunting

Realizar el monitoreo tipo red donde se deberá monitorear la salud de los dispositivos, y servicios definidos por la ENTIDAD, así mismo se deberá realizar monitoreo de eventos tipo SOC (Security Operations Center, por sus siglas en inglés), donde se deberán detectar todas las amenazas cibernéticas que puedan afectar las plataformas tecnológicas.

Se debe garantizar el monitoreo 7x24 del estado y disponibilidad de los activos objeto del servicio SOC y se deben generar las alertas correspondientes en caso de eventos que puedan afectar a la seguridad (confidencialidad, integridad o disponibilidad) de la información o la continuidad de servicio de la plataforma IT de la ENTIDAD, así como de sus procesos misionales. Las alertas por generar, adicionalmente a las que recomienden las buenas prácticas y las predefinidas por la herramienta de SIEM, deberán definirse de acuerdo con el Supervisor del Contrato de la ENTIDAD cuando se detecten oportunidades de mejora.

El CONTRATISTA debe contar y poner a disposición de la Entidad, de un equipo humano certificado, altamente calificado y con amplia experiencia demostrable en temas de seguridad de la información y ciberseguridad y en los servicios requeridos por la ENTIDAD.

Los procesos de gestión y operación deben estar basados en lo posible con las mejores prácticas establecidas por el modelo de procesos ITIL.

Todos los procedimientos deben estar debidamente documentados y presentados al administrador de la Solución que este designado por la ENTIDAD.

El CONTRATISTA deberá definir, establecer y asesorar a la Entidad, en la definición de las políticas y parámetros que se configurarán en la solución de SIEM para la recolección, transporte, agregación, agrupamiento, almacenamiento, respaldo, retención, análisis, correlación, manejo de alertas y visualización, entre otras, de la información relacionada con los eventos que generan y/o almacenan los dispositivos de la Entidad.

El CONTRATISTA deberá realizar el afinamiento y aseguramiento del correcto funcionamiento del SIEM propiedad de la ENTIDAD y de las demás soluciones que provea el CONTRATISTA para cumplir los requerimientos mínimos solicitados por la entidad.

Cumplir a cabalidad con la normatividad vigente de protección de datos personales. Si por efectos de la presentación del servicio el CONTRATISTA requiere acceder, recolectar, almacenar, procesar, respaldar y usar información de carácter personal de los titulares de LA ENTIDAD, el CONTRATISTA deberá demostrar que cuenta con una política interna de Protección de Datos Personales que cumpla con los requisitos previstos en el régimen de protección de datos personales.
Los componentes tecnológicos de la solución adicionales que provea el CONTRATISTA para la prestación de los servicios deberán estar debidamente actualizados y soportados por fabrica durante toda la vigencia del contrato.

Por ningún motivo para el funcionamiento de los mecánicos que provea el CONTRATISTA para el monitoreo, recolección y correlación de eventos, LA ENTIDAD deshabilitará o cambiará la configuración de los controles establecidos en la entidad si esto implica una disminución en su efectividad y funcionamiento.

El CONTRATISTA en conjunto con la ENTIDAD definirá serie de reglas, alertas y notificaciones clasificadas y priorizadas para detectar los eventos de las fuentes que se estará monitoreando, las cuales serán reportarlas a la ENTIDAD cada vez que se encuentre en riesgo los principios de integridad, disponibilidad o confidencialidad de los activos tecnológicos.

2.3 MODELO DE OPERACIÓN

El CONTRATISTA deberá contar con un conjunto de metodologías y procesos que permitirá brindar respuesta oportuna a los riesgos y amenazas que se afrontan día a día en la ENTIDAD. Todos los procedimientos deben estar debidamente documentados y presentados a la ENTIDAD.

Se debe prestar el servicio en el idioma español, para la interacción de las áreas de operación.

El proveedor deberá prestar el servicio acorde al modelo operativo definido en el presente documento y contar con una capacidad operativa para brindar el servicio 7x24 desde las instalaciones del CONTRATISTA.

Los servicios de gestión del SOC realizarán seguimiento 7x24 a los ataques originados desde internet al igual que los originados al interior de la ENTIDAD.

El proveedor deberá realizar periódicamente, según lo establezcan las mejores prácticas, análisis de tendencias sobre los eventos y plataformas monitoreadas.

De forma permanente el SOC realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo a la ENTIDAD, resumiendo los resultados en Boletines o Informes extraordinarios de SOC.

El proveedor deberá contar con un informe detallado sobre alertas mundiales que puedan afectar la seguridad sobre la infraestructura de sus clientes.

El CONTRATISTA debe definir la matriz de escalamiento en común acuerdo con los responsables de seguridad de la ENTIDAD, clasificando el nivel de escalamiento según el tipo y nivel del evento.

El personal del SOC deberá realizar el escalamiento y las comunicaciones por medio de los medios de comunicación establecidos en el alcance de operación, con el personal que designe la Entidad a fin de comunicar las incidencias presentadas y su acción inmediata. Adicionalmente realizará el seguimiento a los eventos hasta que estos sean cerrados adecuada y oportunamente.

El CONTRATISTA deberá registrar todos los eventos e incidentes de seguridad que se detecten, asignarle un número único de identificación con el fin de realizar un seguimiento de las acciones tomadas sobre las respuestas ante los incidentes reportados y llevar estadísticas e indicadores con base en este registro.

El servicio debe contar con un portal web con comunicación segura que permita a la Entidad tener una visualización de la información relevante respecto a amenazas emergentes, vulnerabilidades en su plataforma e incidentes de seguridad detectados por el servicio de SOC.

Los contenidos de este portal web deberán estar orientados a mostrar la información del estado de la operación a nivel de monitoreo, investigación, atención de incidentes y gestión de requerimientos.

El proveedor deberá detallar los procesos de:

a. Servicio de monitoreo y alertamiento.
b. Eliminación segura de la información que ya no se requiera
c. Gestión y Respuesta a incidentes
d. Priorización de incidentes
e. Detección, categorización y alertamiento temprano y oportuno de incidentes de seguridad,
f. Priorización de atención de incidentes,
g. Atención y escalamiento de requerimientos
h. Mejora Continua del servicio
i. Gestión de cambio sobre la plataforma que soporta el servicio.

Control de cambios: El CONTRATISTA deberá seguir el procedimiento de cambios definido en la Entidad, para la instalación, configuración, cambios, actualizaciones y solución de incidentes y/o problemas de los servicios contratados por la entidad, por ningún motivo el CONTRATISTA realizará cambios sobre dichos

servicios, sin que para esto exista el debido consentimiento y aprobación por parte de la Entidad y los mismos se deberán realizar de la forma más eficiente, asegurando en todo momento su calidad, seguridad y continuidad. Todo cambio que realice el CONTRATISTA sobre los servicios contratados debe quedar debidamente documentado.

2.4 DESTRUCCIÓN DE LA INFORMACIÓN DE EVENTO E INCIDENTES DE SEGURIDAD

A solicitud de la Entidad, el CONTRATISTA deberá entregar y/o destruir la información de los eventos e incidentes de seguridad de la Entidad que haya identificado, almacenado y/o gestionado. Para tal efecto, el CONTRATISTA deberá tener en cuenta las siguientes condiciones:

- Deberá entrega a la Entidad la información de los respectivos eventos e incidentes de seguridad de la Entidad que haya detectado, almacenado, gestionado y/o que este en su posesión.

Una vez la Entidad compruebe que la información entregada se puede leer, el proveedor deberá proceder a la destrucción de esta, utilizando para esto mecanismos de borrado seguro que garanticen la eliminación permanente de los datos.

2.5 CANAL DE COMUNICACIÓN

El CONTRATISTA deberá disponer de un centro de monitoreo de seguridad que analice la información, que será entregada por las fuentes que establezca la Entidad a través de canales de comunicación seguros cumpliendo los requisitos de alcance de operación.
Se requiere que la comunicación entre el Centro Principal de Procesamiento de la Entidad y el Centro de Procesamiento del proveedor se realice mediante una conexión segura, teniendo en cuenta para esto las condiciones y parámetros de seguridad establecidos por la Entidad para este tipo de conexiones y de acuerdo con el siguiente esquema:

- La conexión segura se utilizará para consultar y gestionar el SIEM para el proceso de detección, protección.
- La conexión segura (VPN Site to Site) entre el Centro Principal de Procesamiento de la entidad y el Centro de monitoreo, análisis, correlación, respuesta y recuperación de los incidentes de seguridad y procesamiento del CONTRATISTA, se establecerá con el fin de evitar comprometer la seguridad de la información de la entidad que se transmita por este medio y que solo deberá corresponder a información requerida por el CONTRATISTA, para llevar a cabo las actividades de detección, protección, monitoreo, análisis, correlación, respuesta y recuperación de los incidentes de seguridad, El CONTRATISTA deberá tener que cumplir los lineamientos de seguridad establecidos por la Entidad para este tipo de conexiones.
- El CONTRATISTA deberá generar acceso a la plataforma de monitoreo mediante el uso de protocolos seguros y autenticación de usuarios.

2.6 GESTIÓN DE INCIDENTES DE SEGURIDAD

2.6.1 GESTIÓN DE ALERTAS, EVENTOS E INCIDENTES DE SEGURIDAD

El CONTRATISTA deberá realizar la gestión de alertas, eventos e incidentes de seguridad de la información a partir de las siguientes actividades: (i) del monitoreo, análisis y correlación de eventos que realice sobre la información recolectada de los eventos que generen los dispositivos de la Entidad, (ii) del monitoreo permanente que realice de amenazas internas, externas y del ciberespacio que puedan afectar la seguridad de la

información de la Entidad, (iii) de los casos de seguridad que le reporte la entidad, (iv) de otras fuentes internas o externas que reporten situaciones que puedan afectar la seguridad de la información y ciberseguridad de la entidad.

El CONTRATISTA deberá realizar el análisis, escalamiento, reporte y seguimiento de las alarmas, eventos e incidentes de seguridad de la información detectados. Así mismo, deberá actualizarse permanentemente y de manera especializada para que esté al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad y por ende repórtalas de manera oportuna.

La gestión de alertas, eventos e incidentes de seguridad que realice el CONTRATISTA le deberá permitir a la Entidad:

- Que los eventos de seguridad y ciberseguridad de la entidad se detecten y se traten con eficiencia, con el propósito de identificar si los mismos se clasifican como incidentes de seguridad de la información.
- Que los incidentes de seguridad y ciberseguridad de la información de la Entidad se gestionen de forma eficiente, efectiva y adecuada.
- Que se implementen las medidas de seguridad adecuadas en la Entidad con el objetivo de mitigar los incidentes presentados.
- Que los eventos e incidentes de seguridad de la información y ciberseguridad detectados son gestionados por la Entidad de forma eficiente y que los mismos sean tratados hasta su cierre.
- Que la Entidad aprenda de las lecciones que dejan los incidentes de seguridad y ciberseguridad, con el fin de mejorar las medidas y mecanismos orientados a proteger la seguridad de su información a través de los informes y gestión de los incidentes presentados.
- Que la Entidad cuente con un mecanismo estructurado que permita cuantificar y monitorear los incidentes de seguridad de la información y ciberseguridad que se presenten en la Entidad.

El SOC, debe definir la matriz de escalamiento en común acuerdo con los responsables de seguridad en la Entidad clarificando el nivel de escalamiento según el tipo y nivel de incidente al igual que la ausencia de atención a las actividades sospechosas e incidentes previamente declarados. Cuando un evento de seguridad ocurre o está en suceso, el SOC deberá identificarlo y estar en la capacidad de relacionar de forma directa o indirecta con otros eventos de seguridad asociados. Estos, constituyen el conjunto de eventos que permite determinar el patrón de ataque, a este conjunto de eventos finitos se les denomina eventos correlacionados.

El CONTRATISTA deberá clasificar y priorizar las alarmas, eventos e incidentes detectados y analizarlos con el fin de poder determinar sus causas, origen e impacto a la Entidad, basado en las necesidades y prioridades que la Entidad indique.

El SOC deberá contar con un grupo interdisciplinario interno para la atención de incidentes, bajo un procedimiento claro y definido.

El CONTRATISTA deberá contar con un equipo especializado en la gestión de eventos e incidentes de seguridad de la información y ciberseguridad, quien tendrá la responsabilidad de monitorear, detectar, analizar, clasificar y reportar de forma oportuna los eventos de seguridad que identifique.

El servicio de gestión de alertas, eventos e incidentes de seguridad deberá contemplar el escalamiento y seguimiento de los casos detectados de acuerdo con el protocolo que se establezca para tal fin.

El CONTRATISTA deberá definir e implementar el procedimiento de Gestión de Eventos e Incidentes de Seguridad de la información y Ciberseguridad, que incluya, entre otros aspectos, los protocolos, actividades y acciones que deberán seguir, tanto el CONTRATISTA como la Entidad, para el desarrollo de las fases involucradas en el ciclo de vida de la gestión de los eventos e incidentes de seguridad que se detecten durante

la vigencia del contrato. Este procedimiento deberá estar alineado con el procedimiento de gestión de eventos de la Entidad.

El CONTRATISTA deberá contar con los mecanismos, procesos, procedimientos y protocolos y con las herramientas tecnológicas y sistemas de información que garanticen la adecuada gestión, administración, operación y ejecución de las diferentes actividades asociadas al ciclo de vida de la gestión de los eventos e incidentes de seguridad de la información con una metodología basada en la NIST.

Ciclo de vida gestión incidentes de seguridad de la información

- Detección y registro de evento.
- Recolección de evidencias
- Análisis y evaluación del incidente.
- Organización, clasificación y priorización del incidente.
- Declaración y notificación de incidente.
- Contención, erradicación y recuperación.
- Actividades Post-Incidente y generación de reportes.

La notificación de los alertas, eventos e incidentes que realice el CONTRATISTA le deberá permitir a la Entidad: (i) responder a los mismos en forma sistemática, (ii) minimizar su ocurrencia, (iii) facilitar una recuperación rápida y eficiente de las actividades afectadas minimizando la pérdida de información y la interrupción de los servicios.

El CONTRATISTA y la Entidad definirán los medios de comunicación apropiados para la agilidad en la comunicación de los eventos e incidentes de seguridad, como contacto telefónico, correo electrónico, mensajes vía celular y/o chat de contacto.

El CONTRATISTA debe contar con una herramienta para el seguimiento del estado de alertas e incidentes y establecer las responsabilidades, roles y los procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información. Para esto debe disponer de una herramienta de manejo de incidentes de seguridad y asegurar los accesos a dicho servicio mediante el uso de protocolos seguros y autenticación de usuarios. El CONTRATISTA debe proveer acceso a un sistema en línea para seguimiento de incidentes, registro de casos, seguimiento a niveles de servicio, reportes, seguimiento al rendimiento de las plataformas, gráficos y estado de incidentes.

2.6.2 CORRELACIÓN Y ALERTAMIENTO DE EVENTOS DE SEGURIDAD

Los dispositivos tecnológicos de la Entidad generan un **archivo de registro de los eventos** denominados LOGs, los cuales deben ser monitoreados por el CONTRATISTA. El CONTRATISTA debe (basado en su experiencia y bases de conocimiento) diseñar el modelo de recolección de LOGs y arquitectura del servicio, con el fin que se tenga en cuenta al menos los eventos relevantes de seguridad y no impacte la normal ejecución de los servicios tecnológicos que apoyan los procesos de la ENTIDAD.

El CONTRATISTA y la Entidad deben definir y configurar una serie de reglas, alertas y notificaciones clasificadas y priorizadas para detectar eventos e incidentes sobre la plataforma tecnológica que se estará monitoreando y reportarlas a la Entidad cada vez que se encuentre en riesgo los principios de integridad, disponibilidad o confidencialidad de los activos tecnológicos.

El CONTRATISTA debe definir el modelo de conexión de los dispositivos que serán monitoreados; especificar los requerimientos técnicos para cumplir con el servicio a contratar; apoyar y soportar a la Entidad en la conexión, configuración y activación de las conexiones técnicas de los dispositivos a monitorear.
La arquitectura de la solución debe tener en cuenta que no se puede impactar la disponibilidad de los activos tecnológicos CORE de la ENTIDAD, ni de la infraestructura crítica que lo soporta.

Adicionalmente, se debe generar alertas de otras amenazas que puedan impactar a la Entidad, como las identificadas en los reportes de análisis de tendencia de centros internacionales SIRT/CERT y en la base de datos de conocimiento del CONTRATISTA, basado en los casos detectados a otros clientes que tenga el servicio ofrecido.

El CONTRATISTA debe informar de manera prioritaria y alertar sobre los cambios de seguridad, de configuración y críticos que se generen en las plataformas tecnológicas que se están monitoreando. Para esto se debe hacer una tabla de alertas, prioridad, tiempos, escalamiento.

El servicio debe vigilar y alertar cuando hay una interrupción en la recopilación de registros de un dispositivo. En otras palabras, si los registros no son vistos desde un servidor en una cantidad determinada de minutos, generar una alerta.

La herramienta de SIEM debe ser alimentada por fuentes de inteligencia externas de amenazas que contengan listas de reputación (IP) y/o dominios catalogados como sospechosos para la generación de indicadores de compromiso.

El CONTRATISTA debe mantener sincronizados todos los relojes de las herramientas de monitoreo con la hora legal para Colombia, suministrada por el Instituto Nacional de Metrología – INM (http://www.inm.gov.co).

El CONTRATISTA debe realizar un monitoreo a los análisis de tendencia de amenazas y riesgos disponibles en Internet o en centros de respuesta a incidentes (SIRT) que permita informar a la Entidad alertas, tendencias, ataques y amenazas provenientes desde el ciberespacio y puedan afectar la infraestructura o los servicios que la Entidad presta. Asimismo, el CONTRATISTA debe disponer de servicios de Inteligencia ante Ciber Amenazas.

2.7 INFORMES, METRICAS Y TENDENCIAS

El CONTRATISTA deberá elaborar reportes de monitoreo, cambios, alertas, tendencias, gestión, métricas, estadísticas que se entregarán de manera periódica (diario, semanal, mensual, semestral) según requerimiento de la Entidad.

El CONTRATISTA deberá generar reportes de eventos y de análisis de tendencias, para tomar las acciones preventivas y/o correctivas, tales como: instalación de parches, actualización de versiones, modificación de políticas y configuraciones. Además, debe quedar registros de cuándo, dónde y cómo se presentan los incidentes, así como definir nuevos reportes acorde a las necesidades de la ENTIDAD.

2.7.1 Informe Mensual: El CONTRATISTA deberá entregar de forma mensual los respectivos informes y reportes que soporten la gestión y operación del SOC y de los servicios contratados, los cuales deberán contener como mínimo la siguiente información:

- Estado de los equipos o dispositivos monitoreados.
- Principales hallazgos

- Recomendaciones generales
- Herramientas y tecnologías utilizadas
- Estado general de la seguridad
- Tendencias de amenazas observadas
- Top de alertas e incidentes de seguridad, rendimiento y disponibilidad
- Comparativo con periodos anteriores
- Total de eventos registrados
- Clasificación por severidad (Severo, Alto, Medio, Bajo)
- Informe de los incidentes de seguridad presentados con:
    - Descripción
    - Fecha y hora
    - Impacto real y potencial
    - Sistemas afectados
    - Acciones tomadas
    - Riesgos asociados
    - Responsable contactado
    - Estado (Pendiente, en curso, resuelto)
    - Recomendaciones puntuales
- Línea de tiempo de los incidentes presentados.
- Tiempos de respuesta y resolución de incidentes.
- Total de alertas tempranas generadas.
- Casos escalados o desestimados.
- Vulnerabilidades críticas y altas.
- Sistemas afectados
- Recomendaciones específicas.
- KPIs y Métricas clave (MTTR, MTTD).
- Estado de seguridad de la entidad en la deepweb y en la darkweb
- Información de la gestión realizada sobre los requerimientos, casos, eventos o situaciones reportadas por la entidad.
- Acciones que se adelantaron durante el periodo con el objetivo de:
    - (i) Fortalecer los mecanismos de monitoreo y correlación de eventos
    - (ii) Mejorar la gestión de eventos de seguridad.
- Lecciones aprendidas.

- Conclusiones y recomendaciones.

2.8 DETALLE DE LOS RECURSOS TECNOLOGICOS – CASOS DE USO SIEM

2.8.1 GENERALIDADES

El SOC debe estar en capacidad de colectar, procesar, monitorear y correlacionar mínimo 175 fuentes de información a través del SIEM y 300 fuentes de información a través de la herramienta de monitoreo.

Los canales de comunicación (red de datos) se centralizan en la ciudad de Bogotá y el CONTRATISTA será encargado de configurar, operar y administrar la arquitectura tecnológica del servicio de monitoreo.

Para la prestación del servicio de monitoreo de redes y servicios tipo **SOC**, la Entidad cuenta con una plataforma de tipo Next Generation - Security Information and Event Manager - FortiSIEM con una capacidad actual para 175 Dispositivos, 25 agentes avanzados y 1750 EPS) que permite colectar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la ENTIDAD, así mismo deberá usar la herramienta de monitoreo de red propuesta durante la prestación del servicio, si se requiere infraestructura adicional para el cumplimiento técnico del servicio, el CONTRATISTA debe considerarlo en la propuesta sin que esto implique costos adicionales para la entidad.

Se deberán suministrar los medios de instalación de los agentes que se requieran. Una vez la Entidad realice la Instalación, el proveedor deberá realizar la respectiva configuración y certificación de que se está recibiendo eventos y alertas de monitoreo de los dispositivos informáticos de la infraestructura tecnológica de la Entidad, de acuerdo con las reglas ya implementadas. Solo deberá recibir los eventos que se requieren monitorear.

2.8.2 RECURSOS TECNOLÓGICOS PARA MONITOREAR

A continuación, se establece una línea base de dispositivos de la Entidad que el CONTRATISTA deberá tener en cuenta para el diseño e implementación del servicio:

Tipo de Fuente	Cantidad
Firewall	9
Antivirus	3
Controlador de Dominio	4
Base de Datos	100
Servidores Web	90
Switches	9
Enlaces WAN	6
Servidores	150

De igual manera, debe monitorear los recursos tecnológicos que se adquieran durante la vigencia del contrato.

2.8.3 CASOS DE USO

El proveedor debe ofrecer una metodología de análisis ágil y respuesta rápida apoyado en casos de uso, que le permita contar con casos documentados y acciones correctivas adecuadas, tanto para el monitoreo como para la detección de actividades anómalas o intrusivas.

El CONTRATISTA presentará de acuerdo con su experiencia los casos de uso los cuales deberán ser aprobados por la Entidad. El proveedor deberá tener la capacidad de configurar sin límite alguno las reglas de monitoreo, alertas, notificaciones y casos de uso necesarios, para normal operación del servicio de monitoreo de ciberseguridad.

Los casos de uso mínimos requeridos a monitorear son:

- Tráfico desde / hacia sitio con reputación sospechosa
- Actividades asociadas a conexión de escritorio.
- Intentos masivos de autenticación fallidos.
- Cambio de contraseña en horario inusual.
- Autenticación de usuarios en múltiples host.
- Uso de protocolos de gestión hacia/desde internet.
- Uso de protocolos inseguros hacia/desde internet.
- Monitoreo de Disponibilidad de los equipos.
- Monitoreo de Memoria, CPU, Disco.
- Cambios de Configuración.
- Auditoria de Carpetas Compartidas.
- Monitoreo de Paginas a través de transacciones sintéticas.
- Actividades asociadas a la administración de cuentas de usuario final (UserID).
- Cambios no autorizados en recursos tecnológicos críticos.
- Interrupción en el envío de logs.
- Monitoreo de Transacciones sintéticas.
- Actividades de cuentas privilegiadas.
- Modificación de archivos críticos (control de integridad).
- Intentos fallidos de conexión.
- Intentos de autenticación de fuerza bruta.
- Indisponibilidad de los servicios y aplicaciones web.
- Indisponibilidad de los servidores productivos.
- Ataques de malware.

- Ataques de amenazas persistentes.
- Cambios críticos de seguridad o configuración.

2.9 OPERACIÓN, MANTENIMIENTO Y SOPORTE

El CONTRATISTA debe contar con un Centro de Operaciones y de Monitoreo con las capacidades técnicas y humanas requeridas para soportar de manera oportuna y con calidad los servicios y las soluciones de seguridad a contratar objeto del presente proceso de invitación a ofertar.

Todo el personal asignado por el CONTRATISTA para la ejecución del contrato deberá contar con las capacidades necesarias y requeridas para la adecuada prestación de los servicios a contratar por la Entidad.
El **servicio de SOC** deberá ser brindado en el horario de 7x24 para lo cual se deben establecer los respectivos protocolos y mecanismos de comunicación entre las partes.

El CONTRATISTA deberá estar en la capacidad de realizar el diagnóstico de las soluciones propiedad de la ENTIDAD y de las soluciones propuestas por el CONTRATISTA, definir planes de trabajo de mejora continua, de solución de fallos o problemas de desempeño.

Durante la vigencia del contrato el CONTRATISTA deberá realizar por lo menos un (1) mantenimiento preventivo sobre la infraestructura tecnológica de Solawinds, Aranda, y Fortisiem de la Entidad, con el fin de garantizar su óptimo funcionamiento.

2.10 PUNTO DE ATENCION

El contratista deberá disponer de un centro de servicio que permita realizar seguimiento a los incidentes de acuerdo con el procedimiento de Gestión de Eventos e Incidentes de Seguridad de la información y Ciberseguridad definido por el SOC que cumpla con mínimo:

- Uso del Software de Mesa de Servicio de la ANLA para el cumplimiento con el marco de referencia ITIL, donde se puedan registrar casos o incidentes de forma web, correo o teléfono.

2.11 ACTIVIDADES A DESARROLLAR POR PARTE DEL EQUIPO DE TRABAJO

LIDER SENIOR SOC

FUNCIONES	• Liderar al equipo técnico para garantizar la respuesta oportuna de los eventos detectados por el SOC. • Diseñar y definir la arquitectura y requerimientos técnicos de las soluciones que serán gestionadas durante la prestación del servicio. • Revisar e identificar oportunidades de mejora de los procesos y procedimientos establecidos durante la prestación del servicio. • Establecer los controles y algoritmos de operación del canal seguro entre el CONTRATISTA y la ENTIDAD. • Acompañamiento en los procesos de ciberseguridad de la ENTIDAD con el fin de apoyar el fortalecimiento del sistema de gestión de seguridad de la información basado en normativas y buenas prácticas de operación.

	• Brindar recomendaciones para mejorar los controles y procesos existentes basado en los marcos de ciberseguridad como la NIST, ISO 27001, ISO 27032 entre otros • Liderar el equipo técnico del SOC para garantizar una analítica avanzada con respecto a los incidentes de seguridad detectados por la herramienta de monitoreo SOC • Seguimiento de la operación técnica para garantizar la satisfacción del servicio por parte de la ENTIDAD. • Asegurar que el servicio de SOC vaya de la mano con el Sistema de Gestión de Seguridad de la Información definido por la ENTIDAD acuerdo a las políticas de seguridad de la información y mejores prácticas de seguridad. • Participar del comité de cambios con el objetivo apoyar las acciones correspondientes a cambios de infraestructura, desde una visión de estrategia y buenas prácticas de seguridad. • Brindar recomendaciones para el diseño de la arquitectura de seguridad y protección de la información de la ENTIDAD.
UBICACIÓN	• En las instalaciones del CONTRATISTA, requerido bajo demanda por parte de la ENTIDAD

INGENIERO DE IMPLEMENTACIÓN SOC

FUNCIONES	• Realizar el levantamiento de información (Definición de casos de uso, Activos a Monitorear y Matriz de Umbrales). • Realizar la documentación detallada de los activos/usuarios/dominios de información de LA ENTIDAD objeto del contrato para realizar la prestación del servicio. • Afinar el SIEM de la entidad de acuerdo con los casos de uso establecidos. • Liderar la implementación de la herramienta de monitoreo de red y el software de mesa de ayuda • Realizar las configuraciones en el FortiSIEM para garantizar la integración, visualización y monitoreo de los activos establecidos. • Configuración de los activos de información para realizar la Integración con el FortiSIEM - Realizar las configuraciones en los equipos para recibir y centralizar los logs (SNMP, SYSLOG, WMI) • Activación del Servicio en el Centro de Operaciones de Ciberseguridad • Liderar la implementación de los procesos y procedimiento para garantizar la prestación del servicio. • Realizar set de pruebas de operatividad y notificación de eventos, ajustes de falsos positivos, y revisión del todo el modelo de operación del servicio, con el

	fin de garantizar una respuesta y detección continua y oportuna de los riesgos y vulnerabilidades identificadas por el Centro de Operación de Ciberseguridad en los activos de información de la ENTIDAD que hacen parte de los sistemas de información críticos del core de negocio y de alto impacto para la operación. • Realizar la entrega de todas las soluciones de gestión y monitoreo al equipo del SOC para activar el monitoreo. • Realizar documentación del proyecto con el fin de entregar la documentación técnica de la implementación y afinamiento de las soluciones.
UBICACIÓN	• En las instalaciones del CONTRATISTA, con visitas regulares (al menos 3 veces por semana) a la ENTIDAD durante la fase de implementación con el fin de realizar el levantamiento de información y configuración de las herramientas de gestión y monitoreo SOC.

ANALISTA ESPECIALIZADO SOC

FUNCIONES	• Asegurar que el servicio de SOC va de la mano con el Sistema de Gestión de Seguridad de la Información definido por LA ENTIDAD y cualquier mejora implementada de acuerdo a las políticas de seguridad de la información y mejores prácticas de seguridad. • Recibir y dar trámite a los escalamientos de las alarmas o incidencias que por su complejidad, alcance o gravedad los analistas de nivel 1 no puedan resolver y que por eso sean objeto de dicho escalamiento. • Realizar los debidos escalamientos ante los soportes de nivel 3 de los fabricantes o proveedores en caso de que la herramienta de monitoreo de SOC se encuentra en un estado de incidencia o indisponibilidad. • Realizar acompañamiento en la mitigación de amenazas y vulnerabilidades en las herramientas de monitoreo y gestión administradas por el CONTRATISTA. • Colaborar en levantamiento de información de los activos objeto del monitoreo y correlación de eventos. • Documentación de todos los incidentes o eventos que se presenten en la operación del servicio. • Dar el debido manejo a las alertas que generen las herramientas de monitoreo o los propios sistemas de gestión de cada activo objeto de monitoreo. • Proactivamente sugerir las acciones de mejoras y fortalecimientos de políticas. Esquemas, procesos, procedimientos, formatos, arquitectura TI y demás componentes en lo concerniente a la operación de los servicios del SOC.

	• Generación de los insumos documentales necesarios para la fabricación de los informes de incidencias y de seguimiento relacionados con el monitoreo SOC, la gestión de incidentes y demás actividades dentro de la operación del servicio. • Participar del comité de cambios con el objetivo apoyar las acciones correspondientes a cambios de infraestructura, desde el punto de visto de seguridad. • Creación, mantenimiento, afinamiento y mejoras de reglas de correlación, parsing y demás actividades propias de la administración de la plataforma SIEM. • Mantener actualizada la base de datos de configuraciones CMDB de acuerdo con cada activo monitoreado.
UBICACIÓN	Ingeniero especialista ubicado en las instalaciones del CONTRATISTA con un horario 8x5 con disponibilidad 7x24 cada vez que se active un evento de seguridad que deba ser revisado por el nivel 2, requerido bajo demanda por parte de la ENTIDAD.

ANALISTA SOC

FUNCIONES	• Monitoreo de todos los dispositivos, aplicaciones, bases de datos y demás fuentes de información incluidos en sistemas de monitoreo y correlación de eventos. • Realizar un diagnóstico preliminar de las fallas e identificar el(los) activo(s) involucrados, así como los servicios de LA ENTIDAD que se ven impactados con una incidencia o alerta de seguridad y reportarlo de manera oportuna de acuerdo con la matriz de escalamiento establecida por el contratista. • Realizar los respectivos escalamientos ya sea al nivel 2 o al administrador de la infraestructura de seguridad de la información con el fin de ejecutar las respectivas acciones correctivas y/o de mejora que se evidencien en la operación. • Levantamiento de información de los activos objeto del monitoreo y correlación de eventos. • Documentación de todos los incidentes que se presenten en la operación del servicio. • Realizar la gestión correspondiente a las alertas que generen las herramientas de monitoreo o los propios sistemas de gestión de cada activo objeto de monitoreo. • Proponer las acciones de mejoras tendientes a robustecer las políticas, los esquemas, procesos, procedimientos, formatos y demás componentes en lo concerniente a la operación de los servicios del SOC.

	• La operación del equipo de analistas SOC de Nivel 1 debe ser bajo un esquema 24x7 en turnos rotativos. • Generación de los insumos documentales necesarios para la fabricación de los informes de incidencias y de seguimiento que se presenten dentro de la operación del servicio. • Monitoreo del servicio de remediación y seguimiento de vulnerabilidades de todos los incidentes presentados dentro del alcance del servicio.
UBICACIÓN	• En las instalaciones del CONTRATISTA garantizando un monitoreo 7x24, requerido bajo demanda por parte de la ENTIDAD.

2.12 PLAN DE TRABAJO PROPUESTO PARA LA PRESTACIÓN DEL SERVICIO

Las partes definirán un cronograma para la activación del servicio de monitoreo y garantizar el cumplimiento de las actividades dentro de los plazos de ejecución definidos en el plan de trabajo que comprende el afinamiento, puesta en producción y estabilización de los servicios contratados.

El CONTRATISTA deberá desarrollar un plan de pruebas funcionales/técnicas que permita garantizar la correcta operación del sistema integrado en la plataforma tecnológica.

2.13 SERVICIOS DE ETHICAL HACKING Y MONITOREO DE MARCA

2.13.1 SERVICIO DE PROTECCIÓN DE MARCA EN INTERNET

La entidad requiere un servicio de búsqueda de fuentes de posibles ataques; y una vez detectada alguna anomalía, actuar rápidamente para lograr dar de baja estos sitios, perfiles o aplicaciones.

Para este servicio el contratista debe cumplir con las siguientes especificaciones:
El CONTRATISTA debe disponer de un servicio 7x24 durante el periodo de contrato para la identificación de amenazas que puedan poner en riesgo a la infraestructura de la Autoridad Nacional de Licencias Ambientales en fuentes abiertas.

El servicio debe incluir como mínimo el seguimiento de redes sociales y foros (Google, Facebook, Instagram, X, Tiktok) y Blogs, Foros en línea, sitios wiki, sitios de opinión, sitios de noticias y en general sitios indexados de los buscadores.

El CONTRATISTA deberá proporcionar una solución que protege el siguiente dominio y subdominios: ANLA.GOV.CO al monitorear y analizar emails, registros globales de nombres de dominio, sitios web, redes sociales y tiendas de aplicaciones móviles para identificar usos no autorizados. Una vez se identifique un uso abusivo en redes sociales, sitios web, remitentes de emails o cualquier elemento no autorizado se actuará de manera inmediata informando a la entidad y tomando las acciones previamente establecidas.

El servicio deberá estar en la capacidad de proteger mediante el análisis automático de varias fuentes de información, con el fin, de identificar y mitigar los riesgos y amenazas virtuales que puedan afectar la marca comercial de la Autoridad Nacional de Licencias Ambientales y la experiencia de uso de sus usuarios.

El servicio de Monitoreo de Marca ayudará a la **Autoridad Nacional de Licencias Ambientales** – **ANLA** a prevenir que terceros inescrupulosos usen su marca comercial con fines fraudulentos, de suplantación para afectar la reputación del nombre de la entidad o para la organización de algún ataque físico o virtual a la Entidad.

El servicio debe contemplar las siguientes actividades:

- Monitoreo de datos de acceso a la infraestructura interna (credenciales y llaves de código expuestas) e identificación de filtraciones de datos a través de tokens rastreadores únicos e indexables en la web superficial o identificables en filtraciones de Deep y Dark Web.
- El servicio deberá incluir el monitoreo de dominios corporativos y filtración de credenciales (contraseña o Hash) en tiempo real según detección.
- Monitoreo de uso indebido o de forma fraudulenta del activo en websites (dominio web).
- Monitoreo de anuncios patrocinados en los principales motores de búsqueda de la internet (Google y Bing) que utilizan el activo como expresión de búsqueda.
- Monitoreo de uso indebido del activo en perfiles y páginas de redes sociales.
- Monitoreo de aplicaciones falsas utilizando el activo y a disposición en lugares como Google Play, App Store o como APK distribuido en la web.
- Monitoreo del activo o expresiones similares en nombres de dominios en la internet.
- Monitoreo e identificarán promoción de servicios fraudulentos a nombre de la Entidad en los marketplaces reconocidos (Apple, Google, Microsoft, etc.) y en los marketplaces de redes sociales.
- La notificación de los Takedowns se debe enviar a más tardar 2 horas después de generada la alerta.

El servicio deberá realizar el monitoreo e identificación de amenazas en Deep y Dark Web, además de monitorear varias plataformas y grupos donde el volumen de esquemas fraudulentos es enorme.

El servicio deberá incluir la generación de informes mensuales del servicio incluyendo el Monitoreo de Marca en el cual se incluye por lo menos:

- Resumen de las alertas generadas.
- Categorización de las alertas generadas de acuerdo al servicio que las reporta.
- Gestión de los Takedowns realizados.
- Conclusiones y recomendaciones.

2.13.2 SERVICIO DE ETHICAL HACKING

Por medio del desarrollo de pruebas de Ethical Hacking en los diferentes escenarios se espera medir el nivel de exposición al riesgo de la Entidad en cuanto a seguridad informática. Con los ejercicios de Ethical Hacking se pretende evaluar los controles o sistemas de seguridad con los que cuenta la Entidad para proteger los activos informáticos.

Identificar riesgos, vulnerabilidades o fallas de seguridad sobre los servicios de la organización desde una perspectiva externa con o sin privilegios o acceso a las aplicaciones o tecnologías que soportan los servicios.

Evaluar la seguridad de los sistemas frente a un posible ataque, analizando los riesgos procedentes de cualquier atacante externo/interno que pudiera violar la seguridad de los sistemas de información de la Entidad.

Para el caso de aplicaciones y/o infraestructura, este ejercicio de seguridad será realizado con base a los lineamientos del OSSTMM y OWASP el cual realiza una revisión a las vulnerabilidades más comunes sobre los diferentes tipos de aplicaciones e infraestructura.

El contratista deberá generar recomendaciones para mitigar los fallos o vulnerabilidades encontrados acorde con los lineamientos de la organización y con base en los más altos estándares de seguridad y generar un plan de trabajo para la mitigación de los riesgos encontrados.

El contratista deberá realizar (1) ejercicio de ethical hacking para 5 servicios publicados a internet definidos por la **Autoridad Nacional de Licencias Ambientales – ANLA** durante el plazo del contrato, para el efecto entregará:

- Informe técnico de hallazgos con al menos la siguiente información:
- Problemas de seguridad encontrados priorizados por nivel de impacto (CVE)
- Informe con los resultados de los hallazgos
- Anexos de las pruebas
- Recomendaciones para cada una de las fallas encontradas alineados con el estándar internacional ISO/IEC 27001
- En el informe de retest: Información sobre el estado de las vulnerabilidades encontradas
- Conclusiones y recomendaciones generales

3. CARACTERÍSTICAS DEL LICENCIAMIENTO PARA EL SOFTWARE DE MONITOREO DE RED SOLARWINDS

<table>
<tr><th>ÍTEM</th><th>CARACTERÍSTICA</th><th>REQUERIMIENTO TÉCNICO MÍNIMO</th></tr>
<tr><th colspan="3">ESPECIFICACIONES TÉCNICAS</th></tr>
<tr><td rowspan="2">3.1</td><td rowspan="2">DESCRIPCIONES</td><td>
<table>
<tr><th>Ítem</th><th>Licencias</th><th>Cantidad</th></tr>
<tr><td>1</td><td>SolarWinds Server & Application Monitor SAM por un año (del 18 de nov 2026 al 17 de nov 2027) con capacidad para monitorear 50 nodos</td><td>1</td></tr>
<tr><td>2</td><td>SolarWinds Virtualization Manager por un año (del 18 de nov 2026 al 17 de nov 2027) Capacidad de Monitoreo hasta 16 sockets</td><td>1</td></tr>
<tr><td>3</td><td>SolarWinds Database Performance Analyzer for virtualized por un año (del 18 de nov 2026 al 17 de nov 2027)</td><td>15</td></tr>
<tr><td>4</td><td>SolarWinds Network Performance Monitor SL500 por un año (del 18 de nov 2026 al 17 de nov 2027)</td><td>1</td></tr>
<tr><td>5</td><td>SolarWinds NetFlowTraffic Analyzer Module SL500 por un año (del 18 de nov 2026 al 17 de nov 2027)</td><td>1</td></tr>
</table>
</td></tr>
<tr><td><u>VIGENCIA DEL LICENCIAMIENTO DEL SOFTWARE DE MONITOREO DE RED</u>:

La vigencia de la adquisición del licenciamiento de Monitoreo de Red SOLARWINDS debe comprender el periodo de un (1) año, contado a partir del 18 de noviembre de 2026.

La vigencia del licenciamiento a adquirir de SOLARWIND comprende el periodo de un (1) año contado a partir de la fecha de activación.

El CONTRATISTA debe contemplar dentro del licenciamiento, soporte (que incluye mantenimiento) en esquema 7x24 por un año (1).

A efectos de lograr un adecuado monitoreo de los eventos de red y de seguridad desde las instalaciones de la entidad, se debe contar con las herramientas idóneas que permitan adelantar seguimiento en tiempo real, para el efecto y ante la inexistencia de computadores portátiles que permitan un adecuado desplazamiento para realizar tareas de monitoreo, pruebas, y acceso a la red de forma portable, se requiere un computador portátil que supla esta necesidad por el termino de vigencia del licenciamiento de software, el cuál debe cumplir las siguientes características:

• Procesador Intel® Core™ Ultra 7 258V o superior
• Sistema Operativo Windows 11 Pro 64
• Memoria Ram 32 GB LPDDR5X-8533MT/s o superior</td></tr>
</table>

		• Disco Duro de 1 TB SSD M.2 2242 PCIe Gen4 TLC o superior • Teclado Retroiluminado en Español (LA) • Dos Puertos Usb tipo C • Wi-Fi 6 o superior • Bluetooth® 5.3 o superior • Pantalla de 14 pulgadas El CONTRATISTA debe dar soporte telefónico y/o presencial en horario 7x24 en el caso que se presente alguna falla del licenciamiento de software de monitoreo de red atendiendo las solicitudes en un tiempo menor a una hora calendario y dando solución en un tiempo inferior 24 horas calendario El CONTRATISTA debe garantizar las actualizaciones, el parcheo del software adquirido evidenciado a través del portal web habilitado del fabricante.

4. CARACTERISTICAS DEL LICENCIAMIENTO A RENOVAR DEL SOFTWARE DE MESA DE AYUDA ARANDA

ÍTEM	CARACTERÍSTICA	REQUERIMIENTO TÉCNICO MÍNIMO
ESPECIFICACIONES TÉCNICAS		

4.1 DESCRIPCIONES

Ítem	Descripción de Licencias	Cantidad
1	Aranda Service Management Suite (11 Procesos - RF, IM, KM, SACM, SLM, SCM, CHG, PM, REL, SPM, AM) - U.Concurrente (por un año hasta el 17 de nov 2027	19
2	Aranda Service Management Suite (11 Procesos - RF, IM, KM, SACM, SLM, SCM, CHG, PM, REL, SPM, AM) - U.Nombrado (por un año hasta el 17 de nov 2027)	10
3	Aranda CMDB Cis Adicionales - 2000 Cis, (por un año hasta el 17 de nov 2027)	1
4	Aranda Virtual Support U Concurrente por un año hasta el 17 de nov 2027)	3

El CONTRATISTA debe contemplar dentro del licenciamiento, soporte (que incluye mantenimiento) en esquema 7x24 por un año (1).

El CONTRATISTA debe dar soporte telefónico y/o presencial en horario 7x24 en el caso

que se presente alguna falla del licenciamiento de software de monitoreo de red atendiendo las solicitudes en un tiempo menor a una hora calendario y dando solución en un tiempo inferior 24 horas calendario

El CONTRATISTA debe garantizar las actualizaciones, el parcheo del software adquirido evidenciado a través del portal web habilitado del fabricante.

5. TRANSFERENCIA DE CONOCIMIENTO:

ÍTEM	CARACTERÍSTICA	REQUERIMIENTO TÉNICO MINIMO
ESPECIFICACIONES TÉCNICAS		
5.1	**TRANSFERENCIA DE CONOCIMIENTO**	EL CONTRATISTA deberá realizar transferencia de conocimiento en la administración y configuración de la herramienta de monitoreo SOLARWINDS, software de mesa de ayuda ARANDA, y del correlacionador de eventos Fortisiem, así como: • Dos (2) cursos oficiales CISM (Certified Information Security Manager) de ISACA con voucher de certificación incluido • Tres (3) cursos oficiales de Continuidad de Negocio ISO 22301 con voucher de certificación incluido. Para funcionarios de la entidad definidos por el supervisor del contrato.

6. REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

ÍTEM	CARACTERÍSTICA	REQUERIMIENTO TÉNICO MINIMO
ESPECIFICACIONES TÉCNICAS		
6.1	**REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN**	El CONTRATISTA deberá proveer los recursos humanos, técnicos y físicos que disponga para la prestación de los servicios requeridos por LA ENTIDAD, deberán cumplir con las Políticas de Seguridad y Ciberseguridad de la Información definidas por LA ENTIDAD o que se definan a lo largo el contrato, que apliquen en el desarrollo de los servicios contratados. El CONTRATISTA tiene la obligación de contribuir a proteger la seguridad y privacidad de la información de LA ENTIDAD o de terceros que para efectos de la prestación de los servicios contratados deba recolectar, almacenar, procesar, respaldar y usar. El CONTRATISTA establecerá, mantendrá y seguirá medidas técnicas y organizativas apropiadas con el objetivo de proteger los activos de información de LA ENTIDAD a la cual tenga acceso para efectos de la prestación de los servicios contratados, frente a actos accidentales, no autorizados o ilícitos de acceso, revelación, alteración, pérdida o destrucción.

		El CONTRATISTA se obliga a guardar confidencialidad y reserva sobre toda la información que llegue a conocer en desarrollo del presente contrato. En consecuencia, no podrá reproducir en todo o en parte, ni suministrar esta información a terceras personas, ni usarla con fines distintos al propósito del contrato y se encargará de mantener la confidencialidad de la información, la cual es extensiva a las personas a su cargo, siendo responsable frente a LA ENTIDAD por los daños y perjuicios que se generen en caso de que la misma no sea respetada. Así mismo, se obliga a responder hasta de la culpa levísima de la conservación, cuidado y manejo de la información y sólo podrá exonerarse de su responsabilidad mediante la prueba de caso fortuito o de la fuerza mayor. El intercambio de la información reservada o clasificada de uso interno entre LA ENTIDAD y el CONTRATISTA se realizará cumpliendo las políticas de seguridad de la información y protección de Datos personales de LA ENTIDAD, esta última, cuando haya lugar a su aplicación en consideración a la naturaleza de la información objeto de tratamiento. Para el intercambio de información reservada o clasificada de uso interno entre LA ENTIDAD y el CONTRATISTA, se podrá utilizar la solución tecnológica que disponga la Entidad para tal fin o cualquier otro medio seguro, siempre y cuando, se asegure el cifrado de la información en tránsito objeto del intercambio, con el propósito de proteger su confidencialidad e integridad. **Propiedad de la Información** Toda la información relacionada con el negocio de la Entidad que se almacene en los medios informáticos y tecnológicos que hacen parte de la prestación del servicio del CONTRATISTA, son de propiedad única y exclusiva de LA ENTIDAD Toda la información, desarrollo o activo de información que use, procese, almacene, cree, genere, actualice o modifique el CONTRATISTA durante la vigencia del contrato, son de propiedad única y exclusiva de LA ENTIDAD. **Uso de los datos de LA ENTIDAD** Los datos de LA ENTIDAD se utilizarán únicamente para el desarrollo del objeto contractual, incluyendo finalidades derivadas de la prestación de dicho servicio. El CONTRATISTA en ningún caso utilizará los datos de LA ENTIDAD, ni derivará información de ellos, para finalidades diferentes al desarrollo del objeto contractual. Por lo que respecta a las partes, LA ENTIDAD conserva todos los derechos, la titularidad y los intereses sobre los datos. El CONTRATISTA no adquiere derechos sobre los datos de LA ENTIDAD, salvo por los derechos que LA ENTIDAD conceda al contratista para la prestación del servicio. El CONTRATISTA debe asegurar que dará un manejo adecuado y seguro a la información de la entidad a la cual tenga acceso, cumpliendo con las Políticas

		de Seguridad y Ciberseguridad de la Información y la Política de Protección de Datos personales establecidas en LA ENTIDAD. **Revelación de los Datos de LA ENTIDAD** El CONTRATISTA no revelará los datos de LA ENTIDAD a los cuales llegue a tener acceso a ninguna autoridad o tercero, salvo que lo exija la ley. Cuando el CONTRATISTA este obligado por ley a revelar o divulgar la información de LA ENTIDAD a la cual llegue a tener acceso en virtud de una orden legal o requerimiento proveniente de un organismo gubernamental o entidad reguladora, el CONTRATISTA deberá: - Notificar en todo caso a LA ENTIDAD de tal solicitud, inmediatamente se haya dado lugar a la orden y antes de ejecutarla. - Intentar redirigir a dicho ente para que solicite los datos directamente a LA ENTIDAD. - Cooperar con LA ENTIDAD en el caso que la misma decida impugnar la Orden Legal, y así dar un tratamiento confidencial, evitar o limitar la divulgación de la información solicitada El CONTRATISTA deberá reportar de forma inmediata a LA ENTIDAD cuando identifique o se presente algún evento o incidente o una falla, debilidad o vulnerabilidad que afecte o pueda afectar la seguridad y ciberseguridad del CONTRATISTA y/o de la solución que disponga o provea para la prestación de los servicios contratados.

NOTA 1: El contratista/Proveedor deberá garantizar:

1. Que toda la documentación relacionada con la ejecución del contrato (reportes, manuales, certificados, comunicaciones, etc.) se entregue en formato digital, evitando el uso de papel, en línea con los lineamientos y programas ambientales de la ANLA.
2. Que las actualizaciones de software, correcciones y mejoras se distribuyan y ejecuten mediante canales digitales, evitando el uso de soportes físicos o procesos que generen residuos tecnológicos innecesarios (CD y/o USB).

NOTA 2: El proponente con la firma del presente documento se compromete a cumplir con todos los requerimientos técnicos descritos en los estudios previos y el pliego de condiciones y así mismo manifiesta expresamente que cumple con la totalidad de los requerimientos técnicos diseñados y solicitados por la Entidad.

NOMBRE DEL PROPONENTE:
_____

FIRMA DEL REPRESENTANTE LEGAL:
_____

Nombre del Representante Legal:
_____

C.C.:
_____
_____

Autorizo la notificación electrónica a la dirección de correo electrónico_____