RENOVACIÓN SOLUCIÓN ANTIVIRUS TRELLIX CON 1 AÑO DE ACTUALIZACIÓN Y SOPORTE	
FABRICANTE Y REFERENCIA	Marca -Trellix Referencia de la solución Trellix Endpoint Security Suite (TRXE1) y Cloud Workload Security Essentials CWS-E
OBJETO	Contratar la renovación de la solución de antivirus Trellix Endpoint Security Suite (TRXE1), Suite Cloud Workload Security - Essentials - (CWS-E) existentes en la entidad, y adquisición del licenciamiento adicional con soporte técnico por 1 año, de acuerdo con las características y condiciones técnicas definidas.
Cantidad:	Renovación de Tres mil ochocientas (3.800) licencias Trellix Endpoint Security Suite (TRXE1). Adquisición de cien (100) licencias Trellix Endpoint Security Suite (TRXE1). Renovación de ochenta (80) licencias Cloud Workload Security Essentials – (CWS-E). Adquisición de ciento veinte (120) licencias Cloud Workload Security Essentials – (CWS-E).
Características	Actualmente la entidad tiene implementada la solución: **Trellix Endpoint Security Suite (TRXE1)**[1] que es una solución integral que protege, detecta, investiga y responde a las amenazas en los dispositivos y endpoints tanto en entornos locales como en la nube. Utiliza inteligencia artificial, aprendizaje automático y análisis avanzados para ofrecer una protección proactiva y adaptable frente a un panorama de amenazas en constante cambio. Además, permite integrarse con productos de otros fabricantes, facilitando una defensa unificada y flexible. Incluye componentes como Endpoint Security y EDR Endpoint Detection and Response (con capacidades forenses), los cuales, en conjunto, permiten prevenir ataques, priorizar riesgos y automatizar las respuestas ante incidentes de seguridad. **Cloud Workload Security Essentials CWS-E**[2] que es una solución diseñada para proteger las cargas de trabajo y contenedores en entornos de nube pública, privada e híbrida, ofreciendo visibilidad centralizada, detección avanzada de amenazas y automatización en la respuesta. Permite descubrir automáticamente instancias y contenedores, monitorear el tráfico de red y prevenir configuraciones inseguras o accesos no autorizados, apoyándose en inteligencia global de amenazas (GTI) y análisis con inteligencia artificial. Además, brinda visualización de red con microsegmentación, gestión centralizada de políticas, y protección optimizada para entornos virtuales mediante, todo con el objetivo de fortalecer la seguridad multinube y evitar

[1] https://www.trellix.com/assets/solution-briefs/trellix-endpoint-security-suite-solution-brief.pdf
[2] https://www.trellix.com/assets/data-sheets/trellix-cloud-workload-security-datasheet.pdf

	brechas o propagación de ataques dentro de los entornos virtualizados ofreciendo prevención de amenazas para sistemas operativos de servidores (Windows y Linux).
ÍTEM	**Característica Servicios de Soporte por el Contratista**
1	El proveedor deberá realizar la renovación a la solución Trellix Endpoint Security Suite para tres mil ochocientas (3.800) licencias de estaciones de trabajo existentes y deberá proporcionar cien (100) licencias nuevas todas las cuales deberán estar soportadas y gestionadas a través de la consola de administración en nube de la solución.
2	El proveedor deberá realizar la renovación del licenciamiento Cloud Workload Security Essentials (CWS-E), con el fin de mantener activas ochenta (80) licencias existentes y suministrar ciento veinte (120) licencias adicionales. Asimismo, deberá efectuar la implementación correspondiente en el entorno on-premise[3] de la Entidad, garantizando el correcto funcionamiento de la solución en los servidores virtuales Windows y Linux que la Entidad determine.
3	La solución de protección para Servidores virtuales deberá ser desplegada mediante agentes livianos, gestionadas desde un servidor virtual on-premise que actúe como el motor antimalware para todos los servidores, logrando una protección eficiente al eliminar la carga de antimalware dentro de cada servidor individual y mejorando así el rendimiento general del ambiente virtual. (Management Optimized for Virtual Enviroment – MOVE).
4	El proveedor deberá garantizar que, durante la vigencia del licenciamiento (un año), la Entidad cuente con el acceso y los mecanismos necesarios para acceder a las últimas versiones estables, parches y actualizaciones de la solución que sean liberadas oficialmente por el fabricante. Este acceso deberá estar comprendido dentro del licenciamiento y soporte contratados, de manera que la solución pueda mantenerse actualizada conforme a la evolución del producto, sin que sea necesario especificar la versión vigente al momento de la contratación.
5	Realizar las actualizaciones del antivirus según el sistema operativo a que haya lugar de forma automática y programada de las máquinas de usuario final.
6	El proveedor deberá elaborar y entregar al supervisor del contrato, durante el primer mes de renovación del licenciamiento y soporte, un (1) informe inicial de diagnóstico de la solución de antivirus Trellix implementada en la entidad. Dicho Informe deberá incluir un análisis detallado del estado actual de la solución, identificando condiciones, incidentes y amenazas potenciales que puedan afectar la seguridad de los equipos protegidos. Asimismo, deberá contener recomendaciones técnicas sobre controles y acciones de mitigación de riesgos, junto con propuestas de medidas preventivas orientadas a evitar futuras ocurrencias.
7	Soporte técnico post renovación durante el año del licenciamiento (21/12/2025 – 20/12/2026)

[3] ¿Qué es On-Premises? | Supermicro

Durante los tres (3) primeros meses de vigencia del licenciamiento y soporte, el proveedor deberá realizar por lo menos dos (2) visitas semanales de medio día, en las cuales se efectúen revisiones del estado de la consola, configuraciones, actualizaciones, monitoreo, creación o ajuste de reglas y acompañamiento al administrador de la solución asignado por la Entidad.

Cada visita deberá dejar constancia mediante un acta o reporte técnico que documente las actividades ejecutadas, los hallazgos identificados, las recomendaciones formuladas y las acciones sugeridas para su seguimiento.
Asimismo, el proveedor deberá elaborar y entregar informes mensuales al supervisor del contrato, consolidando la información de las visitas efectuadas durante el periodo. Dichos informes deberán incluir un resumen ejecutivo, las principales actividades desarrolladas, incidencias detectadas, acciones correctivas o preventivas implementadas y recomendaciones orientadas al fortalecimiento de la operación y la seguridad de la solución.

A partir del cuarto (4°) mes y hasta la finalización de la vigencia del licenciamiento, el proveedor deberá realizar por lo menos dos (2) visitas mensuales de medio día, manteniendo el mismo esquema de actas por visita y entrega de informes mensuales consolidados.

El contratista durante la duración del licenciamiento deberá garantizar la atención y resolución de cualquier incidente o problema técnico relacionado con la solución contratada, bajo un esquema de soporte 7x24x365, a través de los canales disponibles (telefónico, correo electrónico, acceso remoto o atención presencial, según la criticidad del caso). El servicio deberá ser atendido por personal especializado y certificado en la herramienta, asegurando la continuidad operativa de la Entidad.
Los acuerdos de nivel de servicio (ANS) deberán contemplar como mínimo los siguientes tiempos de respuesta desde el registro del incidente:

- Severidad 1 (Crítica): respuesta inicial en un máximo de 15 minutos.
- Severidad 2 (Alta): respuesta inicial en un máximo de 30 minutos.
- Severidad 3 (Media): respuesta inicial en un máximo de 8 horas.
- Severidad 4 (Baja o consultas): respuesta inicial en un máximo de 1 día hábil.

La clasificación de severidades y la priorización de atención deberán estar acordes con la naturaleza del incidente y la afectación sobre los servicios institucionales.

En función del nivel de cumplimiento obtenido, se aplicará la siguiente compensación en campañas adicionales de sensibilización en ciberseguridad:

NIVEL DE CUMPLIMIENTO ANS	CAMPAÑAS ADICIONALES DE SENSIBILIZACIÓN EN CIBERSEGURIDAD
≥ 90%	0
≥ 80 % y < 90 %	2
≥ 70 % y < 80 %	4
≥ 60 % y < 70 % 6	6

	<table><tr><td>< 60 %</td><td>8</td></tr></table>
	El soporte técnico brindado debe incluir las siguientes actividades: Registro de incidentes y solicitudes: • Listado o reporte generado desde la plataforma de soporte con número de caso, fecha, hora, severidad, descripción y estado. Informe técnico de atención o resolución: • Documento o ticket cerrado que detalle la causa, acciones ejecutadas, tiempo de respuesta, solución aplicada y fecha/hora de cierre. • Obligatorio para incidentes S1 (críticos) y S2 (altos). Reporte consolidado de soporte (mensual o trimestral): • Estadísticas de incidentes atendidos, tiempos de respuesta y resolución, cumplimiento de ANS, causas recurrentes y recomendaciones preventivas. Actas o reportes de atención presencial (cuando aplique): • Evidencia de intervención en sitio, con descripción del trabajo realizado y firma del responsable técnico o supervisor. Bitácora o registro de comunicación con el fabricante (si hubo escalamiento): • Copia o evidencia del caso escalado, con número de ticket y respuesta del fabricante.
	Realizar dos (2) transferencias de conocimiento durante la vigencia del licenciamiento, a mínimo cuatro (4) personas designadas por el supervisor del contrato, sobre instalación, administración y configuración de la solución de antivirus Trellix Endpoint Security Suite (TRXE1) y Cloud Workload Security Essentials. CWS-E, con una duración total de veinte (20) horas por semestre. La Entidad determinará si dichas sesiones se realizan de forma presencial o virtual, según lo considere más conveniente para el cumplimiento de los objetivos del contrato.
	Ejercicio de Red Team sobre la red interna del DANE El ejercicio tiene como propósito evaluar de manera proactiva las vulnerabilidades de la infraestructura tecnológica del DANE mediante la simulación controlada de escenarios reales de ataque. Con ello se busca identificar brechas de seguridad, validar la efectividad de los controles existentes y fortalecer la capacidad institucional de detección y respuesta ante incidentes. **Alcance:** • Simulación de ataques internos y externos. • Evaluación de la infraestructura crítica, sistemas internos y puntos de acceso periféricos. • Identificación de vulnerabilidades y brechas en los controles de seguridad implementados. • Las pruebas se desarrollarán bajo reglas de compromiso aprobadas, excluyendo actividades destructivas o de denegación de servicio.

Metodología y entregables:
El ejercicio se desarrollará en **cuatro fases** dentro del **primer cuatrimestre del año de soporte (enero a abril de 2026)**, con los siguientes productos y tiempos de entrega:

Fase	Actividades principales	Entregable	Periodo estimado
1. Planeación y definición de alcance	- Reunión de inicio. - Definición de objetivos, reglas de compromiso y sistemas a evaluar. - Validación de accesos y coordinación con el equipo de seguridad del DANE.	Acta de inicio y documento de alcance aprobado.	**12 al 16 de enero de 2026**
2. Reconocimiento y análisis de vulnerabilidades	- Recolección de información pasiva y activa. - Identificación de vectores de ataque y vulnerabilidades. - Elaboración del plan táctico de pruebas.	Informe de reconocimiento y vulnerabilidades preliminares.	**19 de enero al 6 de febrero de 2026**
3. Ejecución de pruebas (ataques controlados)	- Simulación de intrusiones internas y externas. - Explotación controlada de vulnerabilidades. - Documentación de evidencias y trazas.	Reporte técnico de hallazgos iniciales.	**9 de febrero al 20 de marzo de 2026**
4. Análisis, cierre y socialización	- Limpieza de evidencias. - Elaboración del informe final con recomendaciones. - Presentación al equipo técnico del DANE.	Informe final técnico y ejecutivo. Presentación de resultados.	**23 de marzo al 10 de abril de 2026**

Duración total estimada: 13 semanas calendario (primer cuatrimestre de 2026).

Confidencialidad:

	Todos los datos, hallazgos, evidencias y resultados obtenidos durante el ejercicio estarán sujetos a estrictas medidas de confidencialidad. El proveedor deberá firmar un acuerdo de confidencialidad y garantizar el resguardo seguro de la información recolectada, evitando su divulgación parcial o total sin la autorización expresa del DANE.
	El contratista deberá desarrollar y ejecutar dos (2) campañas anuales de sensibilización en ciberseguridad, dirigidas a los usuarios finales de la Entidad. Estas campañas se implementarán mediante cursos e-learning interactivos, complementados con tips, charlas virtuales y actividades pedagógicas, con el propósito de fortalecer la cultura organizacional en materia de seguridad de la información y reducir los riesgos que puedan afectar los activos de información institucionales.
Requerimientos técnicos de la solución	
8	**Generalidades** La solución debe ser capaz de ofrecer entre otros: • Consola de administración centralizada • Protección Antivirus/Antimalware/Antiransomware • Capacidades para la ejecución de análisis forense digital • Inteligencia de Amenazas e integración con servicios de reputación (Insight/TIE) La solución deberá brindar protección para equipos con sistemas operativos: • Windows (versiones 10, 11, Server 2012, 2016, 2019 o superiores). • Linux (Red Hat, Oracle Linux u otros equivalentes). • macOS, en las versiones soportadas por el fabricante. El proveedor deberá gestionar la instalación y mantenimiento de las versiones más recientes del producto, verificando la compatibilidad con los sistemas operativos vigentes. El contratista deberá informar al supervisor del contrato sobre nuevas versiones o actualizaciones relevantes dejando registro de la actividad en un informe técnico mensual cuando se liberen versiones estables. El software antivirus no debe interferir con el normal funcionamiento de los equipos. La solución debe permitir la actualización del Endpoint sin interacción por parte del usuario y sin requerimiento de reinicio. La solución debe tener sistema de administración, distribución y actualización centralizada del antivirus desde la consola del administrador del producto e igualmente instalación automática de nuevas versiones del producto y actualización automática de la base de datos de nuevos virus por el término del vencimiento del licenciamiento.

	Brindar soporte correctivo y preventivo de acuerdo con la solicitud de supervisor del contrato en caso de ser necesario por el término del vencimiento del licenciamiento.
9	**Especificaciones Consola de Administración** - La consola debe permitir realizar tareas como la instalación y configuración de la solución, la gestión de políticas de seguridad, y el seguimiento del estado de los dispositivos protegidos - La consola debe poderse instalar ON PREMISE o accederse en modalidad de SAAS según las necesidades de la entidad y sin incurrir en costos adicionales. - La consola deberá soportar los siguientes navegadores de internet: • Google Chrome • Microsoft Edge • Mozilla FirefoxMicrosoft Internet Explorer 11
10	La solución deberá disponer de un módulo generador de reportes que permita a los administradores designados por el DANE configurar, generar y emitir reportes técnicos bajo demanda, con opciones de personalización y exportación en diferentes formatos, de acuerdo con las necesidades de análisis y seguimiento institucional. Los reportes deberán incluir, como mínimo, la información necesaria para reflejar en tiempo real el estado de la red, conforme a los lineamientos acordados con el supervisor del contrato, y deberán contemplar los siguientes aspectos: • **Infecciones:** Detalle de los virus detectados, archivos afectados, fecha y hora del evento, equipos involucrados y acciones ejecutadas por la solución (eliminación, limpieza, cuarentena, entre otros). • **Cubrimiento:** Nivel de actualización y uso de versiones del producto en toda la red, garantizando visibilidad sobre el estado de protección de los equipos y minimizando el riesgo de brotes de virus en máquinas desactualizadas o desprotegidas. • **Tendencias:** Disponibilidad de informes que permitan realizar análisis de tendencias sobre los eventos de seguridad detectados. • **Gestión de accesos:** La solución deberá permitir la creación de múltiples perfiles administrativos con distintos niveles de acceso a la consola, tales como administradores generales, administradores por sitio o revisores sin privilegios administrativos. • **Visibilidad de instalación:** Generación de reportes gráficos que permitan identificar los equipos que no cuentan con el producto instalado. • **Inventario del sistema operativo:** Identificación de la versión del sistema operativo instalada en cada equipo o servidor.

	La solución debe permitir la creación de distintos roles de usuarios dentro de la consola de gestión para el perfilamiento de usuarios con al menos tres (3) permisos: - Uso - Visualización y uso - Permiso completo
11	**Especificaciones Técnicas Antivirus/Antimalware** Debe permitir seleccionar que aplicaciones con una reputación específica deben ser ejecutadas en modo "contenido", es decir que esta funcionalidad no le permitirá realizar ciertas acciones que hayan sido consideradas como maliciosas dentro del sistema operativo La solución deberá poder tomar acciones o de bloqueo o registro según su configuración Debe estar en la capacidad de integrarse y recibir actualizaciones de reputación de un sistema de inteligencia contra amenazas mediante el uso de protocolo abierto de comunicación diseñado específicamente para esta finalidad, con la capacidad de actualizar todas las máquinas del ambiente en tiempo real, sin necesidad de actualizar políticas o comunicarse con la consola de administración.
12	La solución tener una funcionalidad específica diseñada para inspeccionar archivos y actividad sospechosa con el fin de detectar patrones maliciosos mediante el uso de técnicas de "Machine Learning". El agente se debe poder desplegar desde la consola de administración La solución debe contar con mecanismos de protección para no poder ser desinstalada o desactivada por el usuario La desinstalación de la aplicación puede ser protegida mediante contraseñas desplegadas por políticas configuradas por el administrador. El producto Antivirus debe permitir ocultar el icono en la barra de tareas. El producto debe permitir controlar el uso de la CPU para tareas de exploración en demanda.

13	**Especificaciones Técnicas Inteligencia de Amenazas** La solución debe ser capaz de predecir y priorizar amenazas que puedan afectar a la entidad, basados en el tipo de industria, ubicación geográfica, actores y la postura de seguridad La solución debe ser capaz de realizar inteligencia de amenazas en tiempo real. La solución debe ser capaz de definir flujos de trabajo con análisis y contexto que permita tomar decisiones de manera rápida e intuitiva ante amenazas que puedan afectar la entidad. La solución debe utilizar y realizar análisis integral de las amenazas mediante inteligencia artificial. La solución debe suministrar recomendaciones y contramedidas ante las posibles amenazas detectadas La solución debe suministrar información acerca del nivel de riesgo y exposición de la entidad. La solución debe identificar cuál es el impacto de las amenazas en función de la industria o región. La solución debe ser permitir y sugerir la priorización amenazas sobre las cuales el equipo de TI debe prestar atención en la mitigación.
	La solución debe ser capaz de recibir información de inteligencia de al menos 1 billón de sensores a nivel mundial del mismo fabricante de la misma.
Arquitectura y funcionamiento	
14	La solución contratada debe ser basada en cloud, es decir, toda la gestión de datos se debe realizar en la nube, garantizando el aseguramiento y gestión de las máquinas en tierra.
	La herramienta debe permitir la búsqueda de información en tiempo real de distintos elementos dentro del endpoint.
	La solución debe permitir realizar búsquedas específicas en los eventos recopilados y catalogados en la consola centralizada, así como permitir búsquedas en tiempo real de indicadores de compromiso y permitiendo lo siguiente: • Adquisición de datos forenses. • Contención del host. • Generación de eventos y notificaciones. • Aplicación de una política custom con el envío a cuarentena, terminación de procesos.

	La solución debe tener la capacidad de monitorear posibles anomalías en tiempo real y reportarlas a la plataforma para que sean analizadas.
	La solución debe permitir aplicar mecanismos de contención directamente de la consola y sin la necesidad de contar con herramientas de terceros para estos efectos.
	La solución debe utilizar distintos mecanismos de análisis los cuales deben incluir el uso de playbooks, información externa para detectar posibles incidentes dentro del sistema.
	La solución debe utilizar The MITRE Attack Framework para el análisis de posibles incidentes dentro de la organización.
	En el proceso de análisis de un posible incidente, la herramienta debe permitir asignar distintos estados al proceso de evaluación para determinar la etapa en que se encuentra un incidente.
	La herramienta debe permitir la creación de colectores para realizar acciones sobre los nodos.
	La solución debe permitir generar una infraestructura colaborativa entre puntos de protección ya sea a nivel perimetral, contenido, virtual o en los equipos de usuario final que puedan intercambiar información sobre nuevas amenazas detectadas en tiempo real mediante un protocolo abierto diseñado para este propósito.
	La solución debe permitir poner en cuarentena a los hosts comprometidos con el objetivo de evitar movimientos laterales de códigos maliciosos. También pueden detonar acciones como: parar, terminar un proceso, eliminar o modificar archivos, llaves de registro, o ejecutar un script en lenguajes como: C+, VB, Phyton, powershell, CMD)
	La plataforma debe integrarse a una red de reputación basado en el análisis de campañas de ataques de forma que pueda evaluar el impacto en la red y emita las recomendaciones para poder proteger la infraestructura.
	La solución debe proporcionar la capacidad de realizar análisis forenses de estaciones de trabajo/servidores.
	La solución debe proporcionar la opción de investigación y/o análisis forense en su propia consola de administración.
	Debe contar con integración con motores sandbox para el envío de artefactos sospechosos para análisis en la nube.
	La solución debe tener módulos de detección avanzados, como mecanismos de aprendizaje automático para la detección de malware y protección contra vulnerabilidades explotables en aplicaciones, lo que también permite realizar excepciones o personalizaciones de reglas para evitar falsos positivos o incluso para cumplir con las reglas de negocio.
	La solución debe permitir la personalización de las acciones, facilitando así la recolección y análisis de datos durante una investigación.
	La solución debe apoyar el uso de indicadores de compromiso para la presencia de malware y la detección de ejecución. Los indicadores de compromiso deben ser proporcionados por el fabricante y actualizados de forma automática y regular.
	Los indicadores de compromiso deben permitirle identificar al menos las siguientes actividades de amenaza y/o evidencia:

	• Uso no autorizado de cuentas de usuario válidas • Actividad de comando y control • Malware conocido y desconocido • Tráfico de red sospechoso • Uso de programas válidos con fines maliciosos • Acceso no autorizado a los archivos del sistema.
	En el caso de una alerta, la solución debe realizar una captura automática de recursos para el análisis forense. Como mínimo, debe proporcionar la siguiente información: • El usuario inició sesión en la estación de trabajo • Servicios en funcionamiento y puertas abiertas • Cuentas de usuario y tareas programadas • Procesos en ejecución • Subconjuntos de registros de datos relacionados con la actividad reciente • Datos del sistema • Historial de navegadores y descargas • Entradas DNS y ARP.
Reporteria y management	
15	La solución debe proporcionar una visibilidad integral que permita a los miembros del equipo de seguridad discernir e identificar rápidamente el nivel de amenazas detectadas y tener capacidades de detección y respuesta para identificar, investigar y contener equipos de forma rápida y eficiente.
	El panel de control de soluciones debe mostrar al menos las siguientes métricas de detección y contención: número de terminales con alertas, número total de alertas y número de terminales en estado de contención/aislamiento.
	La solución debe permitir la creación de distintos roles de usuarios dentro de la consola de gestión para el perfilamiento de usuarios.
	La herramienta debe permitir la vinculación de procesos mediante mecanismos de trace
	La solución debe permitir la visualización de información en distintos modelos, desde vistas gráficas de los hallazgos hasta el detalle de la información recolectada.
	La herramienta debe permitir visualizar eventos históricos hasta 30 días.
	El contratista debe configurar en la consola informes para ser exportados consistentes con: • Amenazas detectadas en los EndPoints • Equipos infectados con malware • Versiones de los productos instalados en los EndPoint • Estado de conformidad de los productos • Amenazas por categorías • Entre otras De acuerdo con requerimiento del supervisor del contrato y/o administrador de la plataforma, lo anterior con el fin de facilitar el análisis de los eventos en la administración.

16	**Integración**
	La solución debe integrar una herramienta para la gestión de políticas y despliegue ya sea en la nube o desplegada on-premise.
	La solución debe integrarse con diferentes soluciones de correlación tales como SIEM, SPLUNK, o Forti siem, ArcSight vía protocolos API y/o DXL.
	El contratista debe realizar todas las configuraciones y/o desarrollos que se requieran para realizar dicha integración con la solución de antivirus y Forense sin costo adicional para el DANE.
Certificados de Fabricante	
17	El oferente debe ser canal nivel de distribución (Partner) debe contar con certificado en alguno de los tres (3) niveles más altos Platinum, Gold o Silver de la membresía del fabricante Trellix de la solución **Endpoint Security Suite** y debe ser verificable (documento del fabricante donde se pueda corroborar la información). Este documento debe ser expedido por el fabricante de la solución, con fecha no mayor a tres (3) meses anteriores a la fecha límite de recepción de ofertas.
Equipo de Trabajo	
18	Garantizar que el personal designado para brindar el soporte cuenta con experiencia en la instalación, administración y configuración de este tipo de soluciones de antivirus, para lo cual deberá presentar la CERTIFICACIÓN DE PERSONAL IDÓNEO que se describe en el estudio previo.
Entregables	
19	El contratista debe entregar por escrito durante toda la vigencia del licenciamiento al supervisor del contrato el informe mensual de carácter gerencial, donde se evidencie: • Productos Instalados • Indicadores de gestión • Amenazas contenidas y bloqueadas • Métricas con el rendimiento y la efectividad de la solución antivirus, como tiempo de respuesta, detección de amenazas. relacionadas • Vulnerabilidades de seguridad identificadas y corregidas • Resumen de eventos de seguridad relevantes: - Alarmas generadas - Incidentes de seguridad y su resolución.
	Emitir durante toda la vigencia del licenciamiento al supervisor del contrato en el informe mensual recomendaciones de acuerdo con las nuevas tendencias, técnicas, tácticas y procedimientos de amenazas cibernéticas, con el objetivo de cerrar brechas de seguridad y minimizar los riesgos.
	Al finalizar cada visita el contratista debe elaborar y entregar al supervisor del contrato, un informe de servicio que incluya las actividades desarrolladas. De igual forma, deberá indicar dentro del informe si hubo cambios en alguna configuración.

	El contratista debe presentar dentro de los primeros 15 días de ejecución del contrato un cronograma con las actividades y entregables descritas en el contrato con porcentajes de avance y deberá presentar avances mensuales al supervisor del contrato.