Anexo Especificaciones Técnicas
Estudio Previo: 41844

1. OBJETO:
Adquirir licencias, soporte y actualización del software Antimalware TrendAI

1.2 ALCANCE DEL OBJETO:

El Alcance del objeto contractual: comprende los siguientes ítems.

- ✓ Renovar la suscripción de Licencias Endpoint Security Essentials de TrendAI para las estaciones de usuario final
- ✓ Renovar las Licencias de Endpoint Security PRO de TrendAI para la plataforma de servidores de cómputo corporativo
- ✓ Renovar las Licencias Server Protect de TrendAI
- ✓ Renovar las Licencias de TrendAI CyberRisk Exposure Management
- ✓ Renovar Soporte Técnico Especializado

Esto con el fin de propender la correcta operación de los activos de información utilizados por los servidores públicos del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, de acuerdo con los ANS establecidos en las especificaciones técnicas.

2. OBJETIVO GENERAL.

Proteger la infraestructura tecnológica de la entidad (Almacenamiento NAS, Servidores Corporativos, Estaciones de Usuario final) de las amenazas asociadas a Malware

3. OBJETIVOS ESPECÍFICOS.

- ✓ Elaborar un análisis que permita generar unos estudios previos adecuados para obtener la mejor solución del mercado para “Adquirir licencias, soporte y actualización del software Antimalware TrendAI”.

- ✓ Realizar un proceso de compra pública que permita contar con una solución integral antimalware para la plataforma consistente en los equipos de usuario final, servidores y repositorio NAS.

- ✓ Fortalecer las capacidades institucionales de seguridad informática para dar respuesta y mitigar la materialización de riesgos frente a ciber-amenazas.

4. ESPECIFICACIONES TÉCNICAS ESENCIALES

La Adquisición de licencias, soporte y actualización del software Antimalware TrendAI, comprende:

4.1 SOFTWARE Y LICENCIAMIENTO

ITEM	DESCRIPCION	CANTIDAD
1	Renovar la suscripción de Licencias Endpoint Security Essentials de TrendAI para las estaciones de usuario final	8278
2	Renovar las Licencias de Endpoint Security PRO de TrendAI para la plataforma de servidores de cómputo corporativo	614
3	Renovar las Licencias Server Protect de TrendAI	5
4	Renovar las Licencias de TrendAI CyberRisk Exposure Management	8892
5	Renovar Soporte Tecnico Especializado	1

Las Funcionalidades generales requeridas (Antimalware para Endpoints, Servidores de Cómputo y Almacenamiento NAS) se deben mantener mínimo conforme a la solución actualmente implementada.

Las Funcionalidades requeridas para Trend Vision One CyberRisk Exposure Management, se describen a continuación:

- Lista de activos (endpoints, usuarios, workloads, etc.) clasificados por nivel de riesgo (alto, medio, bajo).
- Reporte de vulnerabilidades conocidas (CVE), mal configuraciones en endpoints, servidores o entornos cloud (Cloud One).
- Un índice global de riesgo de la organización (Risk Index Score), basado en amenazas detectadas, vulnerabilidades, actividades sospechosas, configuración débil, etc.

- Usuarios con credenciales comprometidas, comportamientos anómalos o actividades de alto riesgo.
- Evolución del riesgo y postura de seguridad en el tiempo
- Resumen ejecutivo con gráficos, nivel de riesgo general, número de activos afectados, principales amenazas/vulnerabilidades, y tendencias.
- Integración con otras herramientas
- Protección para entornos locales, híbridos y en la nube
- Definición de casos de uso personalizados
- Respuesta automatizada
- Parcheo virtual
- Consola que permita administrar toda la solución integral de Antimalware TrendAI de manera centralizada.
- Consola que permita administrar toda la solución Server Protect de TrendAI
- Consola que permita administrar toda la solución CREM de TrendAI

4.2 SERVICIO DE ACTUALIZACIÓN

- ✓ Contar con un repositorio de distribución local para una correcta implementación, si aplica.
- ✓ Recibir actualizaciones inmediatas de nuevas amenazas por el periodo contratado.
- ✓ La plataforma deberá mantenerse en la última versión estable y se debe realizar acompañamiento para la migración en caso de que sea necesario.
- ✓ Las nuevas funcionalidades integradas en las actualizaciones deben ser notificadas y documentadas al supervisor del contrato de manera oportuna.
- ✓ Migración a nuevas versiones estables de la herramienta.
- ✓ Ante el lanzamiento de una nueva versión de agente o de la consola, se debe proponer un plan de actualización que deberá ser aprobado por la entidad.
- ✓ Las actividades de actualización que se requieran se deberán programar en horarios previamente autorizados por el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, (horarios no laborales) y estos serán desarrollados por el contratista, quien deberá entregar el plan de trabajo respectivo.
- ✓ Las actualizaciones realizadas por el fabricante durante el periodo del contrato deberán estar incluidas en el costo ofertado.
- ✓ Las actualizaciones y migraciones a otras versiones de la herramienta que sean necesarias deben ser informadas y los servicios prestados de instalación deben ser soportados por el contratista durante el periodo del contrato sin que genere costo para la entidad.

NOTAS:

a. Todos los trabajos de actualización de firmware deben ser notificados y documentados por el proveedor con mínimo ocho (8) días hábiles de anticipación,

el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, informará al proveedor si requiere su apoyo, para recibir su debido acompañamiento.

b. Las nuevas funcionalidades integradas en las actualizaciones deben ser notificadas y documentadas al Supervisor del Contrato, con un plazo máximo de Ocho (8) días hábiles después de completada la actividad.

4.3 SOPORTE

- ✓ El Soporte Técnico Especializado y el licenciamiento deben iniciar mínimo en la fecha de inicio de ejecución del contrato en el SECOP II.
- ✓ El servicio de soporte para los incidentes reportados debe ser atendido según los ANS (Acuerdos de Niveles de Servicio).
- ✓ El procedimiento para abrir un caso será detallado en la reunión inicial entre contratista y supervisor una vez se dé inicio al contrato.
- ✓ No se pueden cerrar los requerimientos, casos de soporte o tickets registrados, hasta que el supervisor del contrato autorice. En caso, de que esto no ocurra en los términos establecidos en los ANS del servicio, se seguirá el flujo de proceso establecido por la mesa de ayuda.
- ✓ El servicio de soporte on-site en la ciudad de Medellín, para solucionar eventos de tipo correctivo bajo demanda con un nivel de servicio, será máximo de una hora entre la llamada y la atención.
- ✓ El servicio de soporte debe ser prestado por personal certificado en la solución.
- ✓ Ante cualquier situación que el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, considere pertinente podrá solicitar el escalamiento al fabricante por parte del proveedor.
- ✓ La atención a pesar de ser 5x8 debe haber un acompañamiento en actualizaciones y/o mejoras previamente acordadas con el proveedor, ya que esto no se puede realizar en horario laboral, sin costo para el Distrito de Medellín.
- ✓ Si la solución o herramienta posee problemas que afecten su normal funcionamiento debe haber atención en sitio tiempo completo hasta que entreguen una solución real confiable y estable.
- ✓ Ante cualquier situación que el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, considere pertinente podrá solicitar el escalamiento de la situación particular al fabricante mediante solicitud expresa por parte del supervisor del contrato al proveedor.
- ✓ Brindar los canales para el soporte técnico requerido por el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín
- ✓ La atención vía telefónica, correo electrónico, Soporte Remoto y/o chat por parte del fabricante deberá garantizarse con disponibilidad 5x8, de lunes a viernes de 8am a 12pm y de 1pm a 5pm, durante la vigencia del contrato.
- ✓ Soporte correo electrónico: respuesta a través de un buzón de correo electrónico de soporte informado con anticipación, y deberá ser atendido de acuerdo con la

criticidad del problema, si la dirección del buzón es modificada deberá ser informado esté con anterioridad el cambio.

- ✓ Soporte telefónico: si el número telefónico o los números telefónicos informados cambian estos deben ser especificados con anterioridad, y deberá ser atendido de acuerdo con la criticidad del problema.
- ✓ Soporte Remoto: para conectarse remotamente con el hardware, deberá contar con previa autorización por parte del líder de infraestructura y acompañamiento por parte del especialista antimalware de la entidad, con el fin de garantizar la seguridad y control en el acceso.
- ✓ Soporte por chat: deberá ser atendido de acuerdo con la criticidad del problema, si el chat es modificado deberá ser informado con anterioridad el cambio.
- ✓ Soporte en sitio según los ANS (Acuerdos de Niveles de Servicio) solicitados.

4.4 GARANTIA DE LA SOLUCIÓN

- ✓ Cubrir las garantías pactadas en las especificaciones esenciales.
- ✓ Garantizar la prestación del servicio con las especificaciones de tipo técnico establecidas en el estudio previo y el pliego de condiciones definitivo.
- ✓ Garantizar la disponibilidad de la solución durante la vigencia del contrato.

4.5 TRANSFERENCIA DE CONOCIMIENTO

- Realizar mínimo una transferencia de conocimiento de veinte (20) horas en diferentes sesiones para mínimo diez (10) funcionarios de la entidad, con el fin de fortalecer la apropiación de los diferentes módulos de la solución antimalware por parte del personal designado de la entidad que permita aprovechar de mejor manera las funcionalidades soportadas; estas sesiones pueden ser virtuales y serán agendadas por el supervisor del contrato; previa concertación con el proveedor.

- Realizar mínimo una transferencia de conocimiento de veinte (20) horas en diferentes sesiones para mínimo diez (10) funcionarios de la entidad, con el fin de fortalecer la apropiación del módulo CREM - Cyber Risk Exposure Management de la solución antimalware por parte del personal designado de la entidad que permita aprovechar de mejor manera las funcionalidades soportadas de gestión de la exposición al riesgo cibernético, identificación y priorización de vulnerabilidades, simulaciones de ataque, integración con otras herramientas, protección para entornos locales, híbridos y en la nube, conexión con el lenguaje del negocio; estas sesiones pueden ser virtuales y serán agendadas por el supervisor del contrato; previa concertación con el proveedor.

- Se deberá dar cumplimiento a una reunión mensual, mínimo de dos (2) horas cada una, en las cuales el proveedor indique si se han generado nuevas características

en la solución, la mejor manera de aprovecharlas, brindando orientación frente al tratamiento de amenazas, las modificaciones definidas por el fabricante para su tratamiento y relacione las mejores prácticas a seguir para incrementar la participación y compromiso de usuarios finales.

4.6 REPORTES

- El módulo de reportes debe estar incluido en la solución, sin costo adicional.
- Debe contener reportes predefinidos.
- Permitir la generación de informes dinámicos los cuales pueden ser diarios, semanales, mensuales, etc. teniendo disponibilidad de datos en un servidor local y permitiendo envío automático del reporte.
- La solución deberá permitir generar reportes de las amenazas bloqueadas.
- La solución deberá tener la capacidad de enviar reportes programados por correo electrónico.
- La solución deberá permitir generar reportes de Account Compromise Indicators (análisis del factor de riesgo por cuentas comprometidas).
- Reporte mensual de los activos identificados sin agente de seguridad.
- Top 10 Aplicativos en la nube más críticos accedidos por los usuarios.
- Inventario Aplicativos locales.
- Reporte de las Vulnerabilidades altamente explotables detectadas sobre los activos de la organización a nivel de aplicación.
- Reporte de las Vulnerabilidades altamente explotables detectadas sobre los activos de la organización a nivel de sistema operativo.
- Reporte de las vulnerabilidades de los activos expuestos a internet.
- Reporte de seguimiento a los factores de riesgo que buscan disminuir el índice de riesgo global.
- Reporte de Incidentes sobre Cuentas de Usuario (ataques de fuerza bruta, viajes imposibles, filtración de datos).
- Reporte mensual de la configuración de acciones automatizadas a través de la generación de playbooks que aprovechan las capacidades de análisis de vulnerabilidades del CREM para mitigar el riesgo de las organizaciones que plantean las CVE altamente explotables que incluya entre otros: la detección de correos electrónicos de phishing, entre otros.
- Informe de Evaluación de Postura de Seguridad Actual (Security Posture Assessment Report)
- Informe de Riesgos de Seguridad de la Información.
- Informe de Conformidad Normativa y Regulatoria.
- Informe de Métricas e Indicadores de Seguridad (KPI/KRI).
- Informes Ejecutivos (Mensual o trimestral) (en PDF con gráficos y conclusiones):
    - Objetivo: brindar una visión de alto nivel, comprensible. No entra en detalles técnicos, pero sí muestra impacto, tendencias y nivel de riesgo.

- Informe Descripción. Resumen de amenazas Cuántas amenazas se detectaron y neutralizaron, distribuidas por tipo (malware, ransomware, phishing, etc.). Tendencia de incidentesGráficas que muestren aumento/disminución de incidentes en el mes/trimestre.Top 5 riesgos actuales Áreas críticas: dispositivos sin protección, vulnerabilidades sin parchar, usuarios con comportamiento riesgoso.
- Dispositivos no conformes: Cuántos endpoints no cumplen las políticas (sin agente, con protección desactivada, etc.).
- Resumen de acciones automáticas Número de endpoints aislados, archivos en cuarentena, escaneos forzados, etc.
- Recomendaciones / Acciones sugeridas para reducir riesgo o fortalecer postura de seguridad.

- El proveedor deberá entregar informes mensuales de cada producto de la solución licenciada con las respectivas recomendaciones y los planes de mejoramiento de la solución cuando aplique.
- La plataforma deberá realizar retención de logs mínimamente por 90 días.

4.7 OTRAS CONSIDERACIONES

Las siguientes consideraciones deben estar incluidas:

- Las especificaciones técnicas requeridas son mínimas, por lo tanto, se pueden ofertar mejores características.
- Se debe especificar en sus manuales, datasheets y documentos relacionados si certifica cada ítem de la propuesta.
- La instalación deberá realizarse por personal certificado en el producto de software objeto del contrato.

4.8 ENTREGABLES

- ✓ Certificación de Partners: El fabricante deberá enviar certificado directamente y a nombre de Medellín, Distrito Especial de Ciencia, Tecnología e Innovación, donde faculta al canal como Partners autorizados para venta, implementación y soporte.
- ✓ El proveedor deberá acreditar como mínimo un ingeniero con las siguientes certificaciones expedidas directamente por el fabricante: ·
  - Certified Trend Vision One XDR Professional
  - Deep Security 20 Certified Professional

- ✓ Certificación de garantía de 1 año, expedida directamente por el fabricante, con plazo 8 días calendario a partir de la firma del acta de inicio.

- ✓ Manuales y documentación actualizada de la última versión para la administración, revisión de configuración, parametrización e instalación de la

solución implementada en la Alcaldía de Medellín, plazo 8 días calendario a partir de la firma del acta de inicio.

- ✓ Plan de contingencia para la plataforma, restauración del sistema, plazo 1 mes calendario a partir de la firma del acta de inicio.
- ✓ El contratista deberá suministrar datos de contacto para soporte y un instructivo de cómo generar los casos, plazo 8 días calendario a partir de la firma del acta de inicio; para este punto cabe aclarar que, si algún canal cambia el procedimiento para colocar un soporte, este documento debe ser actualizado inmediatamente.
- ✓ Diagramas de la plataforma y su integración con terceros (en caso de que la integración sea necesaria), plazo 1 mes calendario a partir de la firma del acta de inicio.
- ✓ Diagramas de flujo del diseño del sistema, plazo 1 mes calendario a partir de la firma del acta de inicio.
- ✓ Plan de trabajo para el aprovechamiento del módulo de CREM al interior de la entidad.
- ✓ Cronograma de servicio de soporte preventivo incluida en la solución, plazo 1 mes calendario a partir de la firma del acta de inicio.
- ✓ Arquitectura de la solución, plazo 1 mes calendario a partir de la firma del acta de inicio.
- ✓ Documento que evidencia el Suministro de las licencias.
- ✓ Documento formal indicando la forma como se escalarán los casos de soporte acorde a los ANS (Acuerdos de Nivel de Servicio).

NOTAS.
Todos los entregables y documentos generados en el marco del contrato serán de propiedad del Distrito de Medellín y deben ser en español y todos aquellos documentos producidos o generados por el fabricante, podrán ser entregados en el idioma inglés.

4.9 ACUERDOS DE NIVELES DE SERVICIO (ANS).

- ❖ De acuerdo con su naturaleza, los incidentes de soporte se pueden clasificar como: Críticos, importantes, Normales o menores; por lo tanto, la atención será regida bajo las siguientes prioridades:

    - **Prioridad 1 (Critica):** Situaciones que afecten la prestación de servicios a la ciudadanía de la línea base administrada, que genere falla masiva en la prestación de un servicio de TI crítico, definiendo estos como: SAP, correo, Internet, que afecte la prestación de algún servicio TI a usuarios del despacho del Alcalde.
        - Tiempos de solución: 60 Minutos.

    - **Prioridad 2 (Alta):** Situación que afecte la prestación de servicio TI a Puntos de atención a los usuarios internos (empleados del Municipio de

Medellín) que afecte la prestación de algún servicio TI a usuarios VIP, Falla que afecte el servicio TI en aulas de capacitación, cuando se dicta una capacitación que afecte el tiempo comprometido por los usuarios, evento TI que impida el desarrollo total de las labores de un funcionario del Distrito de Medellín.

- Tiempos de solución: 120 Minutos.

- **Prioridad 3 (Media):** Evento o situación que impida el desarrollo parcial de las labores de un funcionario del Medellín, Distrito Especial de Ciencia, Tecnología e Innovación.
  - Tiempos de solución: 12 horas.

- **Prioridad 4 (Baja):** Instalación o reparación de software no crítico que no soporte las labores del usuario.
  - Tiempos de solución: 40 horas.

- En caso de presentarse retrasos en el cumplimiento de los acuerdos de niveles de servicio detallados anteriormente, que sean atribuibles al contratista y que a juicio del supervisor del contrato pongan en riesgo la continuidad en la prestación del servicio, se procederá a plasmar en informe de supervisión la situación presentada, con el fin de iniciar el correspondiente proceso administrativo sancionatorio a que haya lugar, de conformidad con la normatividad que rige la materia.

Nota: Independiente de la prioridad, si la solución del requerimiento o incidente requiere diagnóstico previo por parte del fabricante, el cumplimiento de los ANS se determinará por los factores respuesta/diagnóstico.