ANEXO 1
FICHA ESPECIFICACIONES TÉCNICOS
N°17065

El proponente deberá cumplir con la totalidad de los ítems exigidos en el presente documento técnico, los requerimientos mencionados en el Alcance del Objeto Contractual, la Codificación del bien, obra o servicio según las Naciones Unidas – UNSPSC y las respectivas certificaciones de estos estudios y documentos previos, además de los requerimientos de los diferentes documentos de perfeccionamiento de este proceso contractual.

No.	DESCRIPCION
1	Servicio de soporte técnico de 3400 suscripciones de EndPoint basadas en la nube con la solución “Sophos XDR User” o equivalente de fabricante y que despliegue actualizaciones. Por un periodo de 12 meses.
2	Servicio de soporte técnico de 300 suscripciones de EndPoint basadas en la nube con la solución “Sophos XDR User” o equivalente de fabricante y que despliegue actualizaciones. Por un periodo de 12 meses.
3	El CONTRATISTA debe suministrar libre de costo para La Gobernación de Antioquia, el acceso a los manuales requeridos para la operación y solución de problemas durante el licenciamiento de las plataformas de EndPoint.
4	El PROPONENTE deberá anexar la certificación del fabricante de la plataforma de Endpoint (EPP), donde garantice la idoneidad y lo respalde para distribuir e implementar la solución.
5	El CONTRATISTA debe contar como mínimo con un responsable certificado en la solución de Plataforma de Protección Endpoint (EPP) para realizar las tareas de la solución.
6	El CONTRATISTA deberá brindar soporte de plataforma de protección Endpoint (EPP) por 12 meses por parte del fabricante, la atención telefónica debe ser en idioma español por personal experto en la solución.
7	El CONTRATISTA entregará al supervisor del contrato, los documentos que acrediten el licenciamiento de la solución de Protección de Endpoint a nombre de la Gobernación de Antioquia.
8	La solución de la plataforma de protección Endpoint debe contar con soporte por un periodo de 12 meses por parte del fabricante, que comenzará a partir del día en que se activen las licencias de acuerdo con el acta de inicio, EL CONTRATISTA debe entregar un documento del fabricante donde certifique el licenciamiento y el cubrimiento de soporte por este periodo de tiempo.
9	El CONTRATISTA debe incluir un procedimiento para el reporte y escalamiento de los incidentes y/o problemas, que incluya línea de atención telefónica en español, plataforma para el seguimiento y control y correo electrónico, 7 días a la semana, las 24 horas del día, los 365 días del año.
10	La atención se podrá hacer por medio de la conexión de VPN que se le asigne al CONTRATISTA a los equipos de cómputo y servidores, en caso de que el acceso remoto no sea efectivo, se debe desplazar un ingeniero certificado al sitio en donde se reporta el problema, para agilizar en el

	diagnóstico y la solución.
11	El PROPONENTE debe anexar a su propuesta, la(s) URL(s) para descargar las fichas técnicas en la página oficial del fabricante, de todos los productos adquiridos, ofrecido donde pueda validarse el cumplimiento técnico de todo lo solicitado. No se aceptarán documentos privados firmados por el comercializador o el fabricante avalando las especificaciones técnicas solicitadas.
12	El CONTRATISTA deberá realizar transferencias de conocimiento teórico-práctico al grupo de seguridad de la información de la Gobernación de Antioquia y de la FLA o a quien consideren, que está conformado a los funcionarios públicos y contratistas del equipo de Seguridad, con una duración de 15 horas, los contenidos a tratar se acordarán con el supervisor del contrato.
13	La transferencia de conocimiento deberá incluir mínimo los siguientes temas: gestión, administración y configuración de la herramienta de antimalware Endpoint y herramientas de auditoría de directorio activo y file servers, contraseñas del directorio activo, identificación de Vulnerabilidades y solución de inteligencia artificial de antimalware sobre aspectos de configuración, administración, monitoreo y reportes avanzados.
14	El CONTRATISTA debe realizar un (1) estado de salud de todas las plataformas tecnológicas del contrato, entregando un informe donde se especifique el estado actual y las acciones de mejora que consideran importantes en realizar.
15	Servicio de soporte en la nube de la herramienta Tenable One, de análisis de riesgos guiados por el contexto, que permite a los equipos de seguridad pasar de un abordaje reactivo tipo 'apaga fuegos' a un enfoque de prevención. Los equipos de ciberseguridad pueden anticipar y bloquear las amenazas antes de que puedan causar daño. La plataforma basada en la nube identifica y evalúa los activos a lo largo de la superficie de ataque para obtener una vista unificada del riesgo cibernético. Activos: 500. Por un periodo de 12 meses de suscripción.
16	Servicio de soporte de una herramienta profesional en seguridad para realizar auditoría del Directorio Activo con alcance de 4 controladores de Dominio. La aplicación debe generar reportes de los cambios en los usuarios, grupos, ordenadores, GPO (Objeto de directiva de grupo) y OU (Consola de administración de Usuarios y Computadoras). Por un periodo de 12 meses de suscripción
17	Servicio de soporte en software de auditoría y análisis en tiempo real de 3 File Servers Windows. Creación, modificación y eliminación de archivos desde accesos autorizados / no autorizados, con análisis forenses detallados de la seguridad y los cambios de permisos a los documentos en sus estructuras de archivos / carpetas y recursos compartidos. Por un periodo de 12 meses de suscripción
18	Servicio de soporte en la nube de 250 suscripciones de una solución de IA (Cortex Palo Alto) que permita identificar ataques sofisticados, sino que también adapten sus defensas para favorecer la mejora constante y prevenir ciberataques futuros. Al correlacionar de forma nativa los datos de redes de alta capacidad, los EndPoints y la nube, que utilice el aprendizaje automático y el análisis para mejorar todas las fases de las operaciones de seguridad, correlacionando de manera automática con la protección perimetral PA. Por un periodo de 12 meses de suscripción

19	Servicio de soporte en la nube del sistema de protección Web Application Firewall (WAF) tienen como función la de proteger sitios Web que tienen transacciones y están expuestos a la Internet, su objetivo es prevenir y anticipar diferentes tipos de ataque a los que pudiésemos ser vulnerables debido a las múltiples amenazas que permanentemente están buscando objetivos para atacar, especialmente entidades financieras y gubernamentales son el objetivo de múltiples actores delincuenciales cibernéticos. La renovación consta de los siguientes componentes tecnológicos del Web Application Firewall: • Renovar 21 licencias para ambientes web. • Renovar ancho de Banda de Enterprise 50Mbps. La solución de seguridad WAF, nos ayuda a mitigar los siguientes riesgos que está expuesta La Gobernación de Antioquia: Acceso a bases de datos y robo o corrupción de datos personales o confidenciales, modificar el código de un sitio web con el fin de cambiar lo que los usuarios ven o visualizar, interceptar datos personales y confidenciales, ataques de Denegación de Servicio (DoS) que deshabilitan la disponibilidad de los servicios, ataques de bots maliciosos que se definen como software malicioso. Por un periodo de 12 meses de suscripción
20	Suscripción de una solución de gestión de contraseñas, los usuarios de las organizaciones por generar, producir, gestionar y actualizar innumerables credenciales. Esto provoca el olvido de sus claves, la sobrecarga de la mesa de ayuda y la creación de contraseñas vulnerables. Suscripción para 3500 Dominios para la Gobernación de Antioquia. Por un periodo de 12 meses de suscripción.
21	El PROPONENTE deberá informar en la propuesta, el fabricante y nombre exacto de la solución ofertada para las herramientas de seguridad Informática.
22	Servicio de suscripción anual para la ampliación de capacidad de ingesta de datos en la plataforma Cortex XDR Pro de Palo Alto Networks, correspondiente a 100 GB. Este servicio permite la recolección, almacenamiento y análisis avanzado de eventos y telemetría provenientes de diferentes fuentes (endpoints, firewalls, servidores, servicios en la nube y otros dispositivos de seguridad), con el fin de fortalecer las capacidades de detección, correlación y respuesta ante amenazas cibernéticas. Por un periodo de 12 meses de suscripción.