FICHA TÉCNICA

Objeto: "PRESTACIÓN DE SERVICIOS DE INSTALACIÓN Y CONFIGURACIÓN DE LICENCIA ANTIVIRUS PARA LOS EQUIPOS DE CÓMPUTO Y SERVIDORES DE LA ALCALDÍA DISTRITAL DE BARRANCABERMEJA"

ÍTEM	CLASIFICACIÓN UNSPSC DEL BIEN	DENOMINACIÓN DEL BIEN	DENOMINACIÓN Y DESCRIPCIÓN DEL SERVICIO	CANTIDAD	TIEMPO (MES)
1	43233200	SOFTWARE DE SEGURIDAD Y PROTECCIÓN	SERVICIO DE PROTECCIÓN DE EQUIPO DE USUARIO FINAL CONTRA CUALQUIER TIPO DE SOFTWARE DAÑINO, COMO MALWARE (VIRUS, TROYANOS, GUSANOS, ADWARE Y SPYWARE.), MACROVIRUS, VIRUS DE SECTOR DE ARRANQUE, PROGRAMAS MALICIOSOS, RANSONWARE, PHISHING, ROOTKIT, PROGRAMAS PUBLICITARIOS, ETC. ESTE SOFTWARE DEBE PERMITIR PREVENIR, DETECTAR Y MITIGAR CUALQUIER INTRUSIÓN QUE TENGA COMO META CAUSAR CUALQUIER TIPO DE DAÑO AL DISPOSITIVO DE USUARIO FINAL Y/O AL INTERIOR DE LA RED LAN O WAN DE LA ENTIDAD, POR 2 AÑOS.	700	1

Las especificaciones técnicas para la adquisición de software de seguridad endpoint (Antivirus/Antimalware) son:

Nombre del servicio	Antivirus / Antimalware (Software seguridad endpoint).
Descripción	Servicio de protección de equipo de usuario final contra cualquier tipo de software dañino, como malware (virus, troyanos, gusanos, adware y spyware.), macrovirus, virus de sector de arranque, programas maliciosos, ransonware, phishing, rootkit, programas publicitarios, etc. Este software debe permitir prevenir, detectar y mitigar cualquier intrusión que tenga como meta causar cualquier tipo de daño al dispositivo de usuario final y/o al interior de la red LAN o WAN de la Entidad.
Cantidad	700 licencias
Unidad de facturación del servicio	Licencia por equipo.
Funcionalidades / Características Mínimas	El software debe estar en capacidad de: Estaciones de trabajo Windows y Mac Servidores de archivos Windows Teléfonos inteligentes y tablets con iOS y Android Control adaptable de anomalías Firewall Protección contra amenazas web, de archivos y de correos Se administra desde un navegador de Internet Solución alojada Colaboración y comunicaciones seguras de Microsoft Office 365 Bloqueador de ataques de red
	Prevención de ransomware y exploits Cloud Discovery Evaluación de vulnerabilidades Protección de dispositivos móviles Análisis de la causa raíz Borrado remoto Control de aplicaciones Administración de parches y cifrado Control web y de dispositivos Data Discovery Protection para Microsoft Office 365 Prevención de los ataques de USB defectuosos

	Cloud blocking EDR (análisis de IoC, respuesta automatizada, aislamiento con un solo clic) Actualización frecuentes y protección con base en firmas para detectar amenazas de malware. Análisis comportamental realizada por vigilantes de sistemas: Que proporcione una protección proactiva contra amenazas que aún no están registradas en las bases de datos de firmas. Protección asistida en la nube: Que brinda una respuesta a sospechas de amenazas. Sistemas de Prevención de Intrusión basado en host (Host-based Intrusion Prevention System- HIPS) con firewall personal, con reglas predefinidas para que reduzcan el tiempo en la configuración el firewall. Control de aplicaciones: Que posibilite que los administradores de TI fijen políticas que permiten, bloquean o regulan aplicaciones (o categorías de aplicaciones). Control Web: Significa que los controles de navegación por endpoínt siguen al usuario, ya sea en la red corporativa o mientras se encuentra en roaming. Control de Dispositivos: Permite a los usuarios fijar, configurar y aplicar políticas de datos con almacenamiento removible y otros controles de dispositivos periféricos, conectados por USB o cualquier otro tipo de bus. Lista Blanca Dinámica: Informes producidos en tiempo real sobre la reputación de los archivos que aseguren que sus aplicaciones aprobadas se encuentren libre de malware y ayudan a maximizar la productividad de usuario. Tecnologías Antimalware: La detección combinada basada en firmas, proactivas y con asistencia en las nube implica protección en tiempo real. Despliegue con Aprovisionamiento Over-the –air (OTA): Permite preconfigurar y desplegar aplicaciones de manera centralizada utilizando SMS. Correo electrónico y PC. Herramientas Antirrobo Remotas: Supervisión de SIM, Bloqueo Remoto, Borrado y Búsqueda evitan el acceso no autorizado a los datos corporativos si un dispositivo móvil se pierde o es robada. Control de aplicaciones para Dispositivos de Propiedades móviles: Monitorear las aplicaciones instaladas en un dispositivo móvil, según las políticas grupales predefinidas. Que incluya un grupo de Aplicación Obligatoria. Que se una única consola de manejo: Desde una misma pantalla, el administrador puede ver y manejar todo el esquema de seguridad: máquinas virtuales, dispositivos físicos y móviles, de la misma manera. Permitir Instalarse remotamente. Utilizar tecnología de red para evitar que las amenazas invadan un punto final. Permitir Actualizaciones de software y de firmas y bases de datos de conocimiento diarias, semanales, mensuales, etc., de acuerdo con las políticas de seguridad de la Entidad y del fabricante del software adquirido. Permitir la configuración mediante reglas o políticas de protección, de acuerdo con las necesidades de la Entidad. Utilizar filtro de sistemas de archivos para evitar que las amenazas se escriban en el disco. Prevenir la perdida de información. Permitir el cifrado de datos almacenados en archivos, directorios, discos, almacenamiento externo y dispositivos extraíbles. Contar con una consola de administración centralizada instalable donde indique la Entidad compradora (en sitio, nube pública, nube privada, o instalaciones que hagan parte de la infraestructura tecnológica de la Entidad Compradora). Protección activa/pasiva en tiempo real. Evitar que cualquier amenaza de día cero o desconocida que suceda o pase, dañe la infraestructura de TI. Detectar y eliminar en tiempo real cualquier tipo de software dañino, malware (virus, troyanos, gusanos, adware y spyware.), macrovirus, virus de sector de arranque, programas maliciosos, ramsonware, phishing, rootkit, programas publicitarios, así como las aplicaciones potencialmente no deseadas.

	Proteger contra amenazas desconocidas en tiempo real. Asegurar que todos los archivos almacenados y las unidades externas de almacenamiento (CD, DVD, memorias USB, discos externos, etc.) no tengan amenazas. Acceder a la inteligencia de amenazas global del fabricante en tiempo real. Mantener el equipo (endpoint) en excelentes condiciones de rendimiento para no interferir con las labores diarias del usuario. Proteger contra amenazas y virus en internet en tiempo real y sobre cualquier navegador. Contar con módulo de firewall de usuario final, programable desde consola o desde usuario final. Soportar protocolos IPv4 e IPv6. La solución debe permitir la integración con el directorio activo de la Entidad y ser compatible con todas las configuraciones del mismo. La solución debe permitir la integración con herramientas de análisis forense de externos de acuerdo con las necesidades la Entidad. La herramienta de software debe contar con una protección general contra aplicaciones y código no deseado, permitiendo sean agregadas en listas blancas o listas negras, acorde con las necesidades de la Entidad. La consola de administración debe permitir la exploración de la infraestructura de TI de los equipos a los que se instala el Antivirus / Antimalware (Software seguridad endpoint), para generación de inventarios de dichos activos. Permitir el manejo de fallas y contingencia del software instalado. La herramienta de software debe contar con los mecanismos de seguridad propios que eviten la desinstalación o inactivación por parte del usuario final. La herramienta de software debe permitir realizar escaneos programados o por demanda; desde la consola de administración o desde la consola del usuario final. La herramienta de software debe permitir configurarse con acciones para atender alertas o infecciones identificadas (Bloquear, limpiar, eliminar, enviar a cuarentena, ninguna). La herramienta debe alertar sobre una posible infección por las diferentes vías de entrada tales como internet, correo electrónico, red, dispositivos USB o discos extraíbles.
Plataformas soportadas	La herramienta deberá estar en la capacidad de poderse instalar como mínimo en computadores de escritorio, servidores, tables, estaciones de trabajo y portátiles con sistemas operativos: Windows 32 y 64 bits IOS Android Y la herramienta deberá poseer compatibilidad con los siguientes navegadores: Microsoft Edge Firefox Google Chrome Microsoft Edge Safari (para Mac)
Hardware	La herramienta deberá estar en la capacidad de poderse instalar como mínimo en computadores de escritorio, servidores, tables, estaciones de trabajo y portátiles con las siguientes características mínimas: 4 GB de RAM. 512 GB de espacio libre en el disco duro. Procesador de 2 GHz, mínimo de dos núcleos físicos.
Tiempo de vigencia del licenciamiento	Opciones de licenciamiento por: Dos (2) años. A partir del vencimiento del tiempo de licenciamiento, el software quedará en la Entidad, pero no permitirá su actualización en la herramienta y en su base de datos.
Reportes / Informes	La consola de administración debe permitir la parametrización, generación, consulta y exportación de informes o reportes de acuerdo con las necesidades de la Entidad, dichos reportes como mínimo deben estar relacionados con la instalación, funcionamiento y fallas del software instalado.

	Los reportes o informes deben y pueden ser parametrizables de acuerdo con las necesidades de la Entidad.
Idioma	La herramienta debe permitir la configuración en el idioma español, tanto en usuario final como en la consola de administración.
Capacitación	El Proveedor capacitará a máximo cuatro (4) usuarios que la Entidad defina, en el uso, instalación y administración del software adquirido, con una intensidad de mínimo dieciséis (16) horas distribuidas en máximo cuatro (4) sesiones. Dicha capacitación se realizará presencial o remotamente.
Soporte Técnico	El proveedor deberá estar en la capacidad de prestar soporte remoto 24/7 para la herramienta por el tiempo de adquisición de esta, este requisito no ocasionará costo adicional para la Entidad.
Canales de atención	El Proveedor debe contar como mínimo con los siguientes canales de atención a requerimientos: Telefónico Correo electrónico
Entrega e instalación	El Proveedor deberá entregar instaladas la(s) 700 licencia(s), contratadas, la consola administración configurada, con todas las reglas y políticas, de implementación configuración y puesta en marcha de la herramienta. La instalación puede ser remota o en sitio
Soporte	Soporte remoto o presencial con ingeniería certificada 5/8

NOTA. EQUIVALENCIA FUNCIONAL: Las denominaciones comerciales incluidas en esta ficha técnica se entenderán como referencias a las funcionalidades requeridas y admitirán su equivalente funcional. Los oferentes podrán presentar propuestas técnicas con productos de cualquier fabricante, aun cuando utilicen denominaciones diferentes, siempre que cumplan la totalidad de las condiciones mínimas, el alcance y el nivel de protección exigidos por el Municipio. La equivalencia deberá acreditarse mediante documentación técnica del fabricante que permita verificar el cumplimiento de cada funcionalidad requerida.

LUIS EDUARDO CRUZ GONZÁLEZ
Director de Servicios Administrativos

	NOMBRE DEL FUNCIONARIO	FIRMA	FECHA
Proyectó:	John E. Lozano		
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			