Anexo Técnico No. 1 Especificaciones Técnicas

Objeto: Adquirir la suscripción del licenciamiento y soporte de antivirus para proteger la información y mitigar amenazas informáticas en los equipos de cómputo y dispositivos de la SDH.

ITEM	DETALLE	REQUERIMIENTOS TECNICOS MINIMOS
1.	ESPECIFICACIONES DEL SOFTARE	Adquisición de 1.800 licencias de seguridad con capacidades avanzadas de Extended Detection and Response (XDR), incluyendo funcionalidades de protección de endpoints (EDR), soporte técnico y actualizaciones por un periodo de 12 meses.
		La solución de seguridad deberá ser de tipo corporativo, no admitiéndose soluciones de uso doméstico, y deberá contar con capacidades integradas de EDR (Endpoint Detection and Response) y XDR (Extended Detection and Response) orientadas a la detección, correlación, análisis y respuesta ante amenazas avanzadas. La solución deberá garantizar monitoreo continúo basado en comportamiento, detección de amenazas, registro de eventos para análisis forense, generación de alertas en tiempo real y capacidades de respuesta como aislamiento de equipos y bloqueo de procesos. La solución deberá correlacionar alertas y eventos de endpoints, identidad/Active Directory y aplicaciones cloud soportadas, y permitir integración con SIEM/herramientas externas. La solución deberá administrarse centralmente desde la consola cloud del fabricante para políticas, dispositivos, alertas y respuesta; las integraciones del ecosistema podrán operar desde servicios del fabricante integrados a la consola.
		La solución deberá ser suministrada bajo el modelo de servicio en la nube Software as a Service (SaaS), alojada y operada íntegramente sobre la infraestructura del fabricante. Este será responsable de la administración, operación, mantenimiento, actualización, disponibilidad y seguridad del servicio. La entidad dispondrá de acceso a las funcionalidades de administración del producto para su gestión y configuración, sin requerir infraestructura local.
		Actualización automática para los endpoint y gestión de manera manual y/o programada desde la consola de administración por el término de vigencia del licenciamiento.
		Instalación de la última versión estable de la solución de seguridad con capacidades de *Extended Detection and Response (XDR)*, incorporando funcionalidades avanzadas de protección de endpoints (EDR), así como detección y respuesta centralizada ante amenazas, para estaciones de trabajo, servidores y consolas de administración.
		La plataforma debe activar una integración extendida que correlacione actividad del usuario en aplicaciones cloud con incidentes de detección y respuesta en endpoint.
		La solución deberá aplicar políticas de navegación web y control de acceso desde el endpoint y consola cloud, incluyendo usuarios remotos mediante el agente instalado.

		La plataforma debe permitir definir restricciones para dispositivos, puertos y medios extraíbles, reduciendo fuga de datos o introducción de malware por canales físicos. Debe facilitar excepciones controladas, auditoría de eventos y alineación con políticas de seguridad corporativa sin desplegar una herramienta adicional aislada.
		ante actividad maliciosa que modifique, elimine o cifre archivos, la solución deberá detectar el comportamiento, detener el proceso atacante y ejecutar automáticamente la reversión de las acciones realizadas por el código malicioso, incluida la recuperación de archivos afectados desde un repositorio o caché local protegido. La capacidad deberá administrarse desde la consola central, operar sin depender de una plataforma externa de copias de seguridad y mantenerse disponible durante toda la vigencia del licenciamiento
		La solución debe permitir que los equipos de seguridad contengan endpoints comprometidos y neutralicen artefactos maliciosos desde la consola, reduciendo el tiempo entre detección y remediación. Estas acciones deben quedar auditadas y vinculadas al incidente para soportar investigación, cumplimiento y mejora continua.
		La consola de administración debe realizar las actualizaciones programadas sobre los computadores y servidores que se encuentren en la red por el término de vigencia del licenciamiento.
		La consola debe permitir delegar administración por responsabilidades, segmentar dispositivos por unidad de negocio, aplicar políticas diferenciadas y mantener trazabilidad de cambios. Debe estar disponible en la consola cloud del mismo fabricante para evitar consolas separadas.
		Desde la consola se debe administrar en cada uno de los endpoint y/o grupos, la actualización de los clientes, en su versión de antivirus, actualización de los archivos, servicios de definición y/o firmas de virus, motor de búsqueda, parches y actualizaciones extraordinarias por el término de vigencia del licenciamiento.
		Ante un nuevo virus el fabricante debe ofrecer un protocolo de seguridad y un servicio de recuperación de daños por el término de vigencia del licenciamiento.
		Los productos objeto de esta contratación, deben estar en capacidad de actualizar automáticamente las políticas de prevención, las vacunas o patrones sin congestionar la red, ni afectar el rendimiento de las estaciones por el término de vigencia del licenciamiento.
		La solución de antivirus debe generar reporte de los virus detectados y acciones realizadas al respecto por el término de vigencia del licenciamiento.
		El fabricante debe proveer un servicio proactivo para determinar e implementar políticas de prevención ante nuevos ataques, que se aplique a los productos en forma automática y centralizada por el término de vigencia del licenciamiento.
		El software antivirus debe permitir cifrado de información confidencial por el término de vigencia del licenciamiento.
		Control de aplicaciones: Control de privilegios de aplicaciones que controle la actividad de estas para el uso de recursos informáticos. Brindar la posibilidad de monitorear y controlar las aplicaciones, permitir y denegar el acceso a determinadas llaves del registro, archivos y carpetas. Debe tener la capacidad de agregar software a una lista de “aplicaciones confiables”, donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas.

		Control de Dispositivos: Control por tipo de dispositivo a ser conectado. Permitir a los usuarios seleccionados y / o grupos de usuarios acceder a determinados tipos de dispositivos durante períodos específicos de tiempo.
		Control de Navegación: Control de acceso web para usuarios y / o grupos de usuarios. Control de acceso web mediante filtros. Control de acceso web mediante filtro por tipos de archivos. Control de acceso web mediante filtro por direcciones URL.
		La funcionalidad debe permitir que los eventos de seguridad no se analicen de forma aislada, sino como parte de una cadena extendida que incluya usuario, dispositivo y aplicación cloud. Con el fin de fortalecer la detección de compromiso, abuso de cuentas y exfiltración, especialmente cuando la actividad maliciosa de manera cruzada endpoint y nubes. Debiendo correlacionar todos los eventos tanto de los endpoint como de la actividad nube del usuario en la plataforma XDR de manera nativa.

		El agente deberá integrar protección endpoint, EPP+EDR/XDR, control web, control de dispositivos, cifrado, soporte y operación coordinada.
		La solución debe incorporar motores de machine learning entrenados con inteligencia global de amenazas para evaluar archivos, reputación, atributos, comportamiento y contexto de ejecución antes o durante su actividad en el endpoint. Esta capacidad debe complementar el análisis tradicional antimalware, reputación en la nube y análisis conductual, permitiendo bloquear amenazas nuevas sin depender exclusivamente de firmas estáticas
		Borrado Remoto: La solución deberá contar con un componente en el endpoint que permita la eliminación remota, inmediata, silenciosa y auditable de información corporativa seleccionada o, cuando las políticas de la SDH así lo determinen, de la información contenida en el dispositivo. La acción deberá ejecutarse sin interacción del usuario final una vez el endpoint reciba el comando emitido desde la consola central de administración de la solución. La ejecución de la funcionalidad estará sujeta a que el dispositivo administrado cuente con conectividad para la recepción de políticas y comandos remotos.
		El agente o cliente de la solución deberá ser liviano y eficiente en el uso de recursos, garantizando un consumo optimizado de CPU, memoria y almacenamiento, de manera que no impacte negativamente el desempeño, estabilidad ni la experiencia de usuario en los equipos de la entidad, tanto en condiciones de operación normal como durante procesos de análisis o actualización.
		Para las actualizaciones de software el contratista comunicará a la Secretaría Distrital de Hacienda la disponibilidad de nuevas versiones, una vez estén liberadas en su versión más estable (No se instalarán versiones Beta en la Entidad). Se debe garantizar acceso a todas las actualizaciones de versiones de software durante la vigencia del contrato mediante herramientas en línea y contar con medios magnéticos físicos de ser necesario.

		El proveedor deberá garantizar que los productos cubren los diferentes sistemas operativos de la Entidad.
		Gestión de parches y vulnerabilidades: Generación de informes de amenazas de vulnerabilidad en las aplicaciones, con puntuaciones o niveles de severidad que ayudan a adoptar decisiones para protección de las estaciones. Desplegar a través de la solución, los parches o actualizaciones que remedien las vulnerabilidades detectadas.
		Los costos por la solución a problemas ocasionados por la nueva versión de instalación de software los cubre el Proveedor sin costo para la Secretaría Distrital de Hacienda. El trabajo de actualización de software se realizará programado de común acuerdo entre las partes y en horario no hábil donde no afecte el normal funcionamiento de la Entidad de ser requerido.
2.	**CONSOLA DE ADMINISTRACIÓN ANTIVIRUS**	La consola de administración, debe ser único punto de administración y control de todos los productos de la solución.
		La consola de administración debe informar mediante reportes los virus o amenazas que fueron detectadas, identificar los archivos y computadores donde se presentó el evento y las acciones realizadas por el antivirus para controlar la amenaza por el término de vigencia del licenciamiento.
		La consola de administración debe permitir realizar, implementar y gestionar políticas de prevención de amenazas, así como también actualizar las firmas en forma automática e incremental.
		La consola de administración debe permitir realizar escaneos simultáneos, programados o manuales a todos los equipos de la red, (por grupos o de manera individual), por el término de vigencia del licenciamiento.
		La consola de administración debe permitir realizar la administración y aplicación de políticas antivirus, a través de protocolo TCP/IP, por nombre de máquina, usuario, administración por direcciones IP.
		La consola de administración debe informar el estado actual de los equipos administrados.
		La consola de administración debe implementar políticas de seguridad en forma centralizada, tales como: bloqueo de puertos de las estaciones, bloqueo de carpetas compartidas, denegación de permisos de escritura, control de aplicaciones.
		El contratista deberá hacer una presentación de las nuevas funcionalidades que el fabricante libere en la versión actualizada con el fin de que, si la Entidad lo requiere, se adopten y entren en operación. Estas implementaciones las realizara el contratista con el acompañamiento de los funcionarios que la Entidad designe como administradores del software.

3.	**RESPALDO DEL FABRICANTE**	El contratista se obliga a escalar ante el fabricante de la solución, o a través de canales especializados autorizados, los casos que lo requieran, garantizando en todo momento la calidad del servicio. Para ello, deberá contar (directa o indirectamente) con personal calificado y debidamente entrenado para la atención y soporte del software, así como para la gestión y efectividad de la garantía frente a fallas y/o errores reportados, de carácter preventivo o correctivo, asegurando una solución oportuna y satisfactoria durante todo el período de vigencia del licenciamiento.
4.	**PUESTA EN OPERACIÓN, PRUEBAS Y ACEPTACIÓN DEL SOFTWARE ANTIVIRUS**	El contratista deberá realizar la puesta en operación integral del software antivirus, incluyendo la instalación, configuración, parametrización y despliegue de la solución en los equipos y/o dispositivos definidos por la Entidad, garantizando su correcta integración con la infraestructura tecnológica existente y la gestión centralizada a través de la consola de administración. El contratista deberá ejecutar y documentar las pruebas técnicas y funcionales necesarias para verificar el adecuado funcionamiento de la solución, la correcta aplicación de las políticas de seguridad, la actualización de firmas y motores de detección, así como la correcta comunicación con la consola de administración. Superadas satisfactoriamente las pruebas, el contratista deberá elaborar y suscribir el acta de puesta en operación y aceptación del servicio, previa validación y visto bueno del supervisor del contrato. El contratista deberá brindar acompañamiento técnico durante la fase de estabilización inicial, atendiendo incidentes, realizando ajustes de configuración y apoyando la validación del funcionamiento óptimo de la solución. Las actividades descritas en los numerales anteriores deberán ejecutarse dentro de un plazo máximo de **quince (15) días calendario**, contados a partir del acta de inicio del contrato, garantizando que la solución quede operativa y en condiciones óptimas de uso, conforme a los requerimientos técnicos establecidos. El contratista deberá realizar la desinstalación de agentes anteriores de otros productos en los endpoint (o que no corresponda a la versión actualizada) y realizar la instalación del nuevo agente del producto que resulte favorecido en el proceso contractual.
5.	**SOPORTE**	El servicio de mantenimiento preventivo se realizará mensualmente y será programado por la entidad en un cronograma específico. Las actividades que se deben realizar como mínimo en el mantenimiento preventivo son: **a.** Verificación de los productos, **b.** Verificación y/o ajuste de parámetros de configuración de la herramienta. **c.** Ajustes de los reportes de información programados. Los mantenimientos se programarán con el supervisor del contrato en un horario que no afecte la operación normal del servicio de la entidad, garantizando el correcto funcionamiento y operatividad de los productos y de la plataforma informática de la entidad.

		Soporte telefónico: El contratista deberá garantizar acceso al centro de soporte telefónico del fabricante según la modalidad requerida para el software. El contratista deberá entregar un documento donde informe los niveles de escalamiento con todos los datos necesarios para garantizar el soporte. Registro y seguimiento de solicitudes: La Secretaría Distrital de Hacienda recibirá del contratista un número de registro de llamada (TICKET) y deberá contar con un mecanismo sistematizado para efectuar seguimiento y escalamiento de solicitudes en el centro de soporte. El ticket será utilizado por la Secretaría Distrital de Hacienda para realizar un control Modalidad de atención: La solución deberá incluir soporte técnico 8x5 con atención al siguiente día hábil (NBD). Para incidentes críticos relacionados con amenazas activas, indisponibilidad generalizada o necesidades inmediatas de contención, deberá garantizarse atención y escalamiento 7x24 a través del contratista y del soporte oficial del fabricante. El soporte se prestará cada vez que la Secretaría Distrital de Hacienda lo requiera, y contempla la atención y diagnóstico de fallas de manera remota, por parte de personal calificado. La Secretaría Distrital de Hacienda reportará la falla por medio de la línea de "Servicio de soporte técnico especializado" con el que debe contar el proveedor, dicho procedimiento de servicio de soporte y escalamiento se debe anexar junto con el contrato de fabrica suscrito.
6.	**PERSONAL CALIFICADO**	El contratista deberá disponer de personal técnico certificado en la solución de seguridad ofertada, con certificaciones oficiales vigentes emitidas por el fabricante o entidad autorizada, que acrediten competencias en instalación, configuración, administración y soporte.
7.	**GARANTÍA**	El contratista debe garantizar la calidad e idoneidad del servicio por el término de vigencia del contrato.
8.	**ENTRENAMIENTO**	El proponente deberá realizar entrenamiento avalado por el fabricante con una intensidad horaria mínimo de 32 horas, para mínimo cinco (5) funcionarios de la Entidad, en la versión y funcionalidad de los productos recibidos. Los entrenamientos deberán dictarse por entidades acreditadas y personal certificado por el fabricante de los bienes ofrecidos y entregando certificación del entrenamiento.
9.	**MATERIAL DE APOYO**	Serán entregados por parte del contratista al supervisor del contrato o a quien el designe, los Instaladores y links de manuales del fabricante para realizar la consulta vía WEB. Se tendrá acceso a las bases de datos de conocimiento con las que cuente el fabricante del antivirus.

10.	**ACREDITACIÓN DEL CONTRATISTA**	**El proponente deberá adjuntar con su oferta una certificación vigente expedida por el fabricante de las licencias de Endpoint, que acredite al proponente en uno de los dos niveles más altos del programa de canales delfabricante ofertado.**
11.	**VERIFICACIÓN DE CUMPLIMIENTO**	**El proponente deberá acreditar el cumplimiento de cada requisito técnico mediante documentación oficial o enlace web del fabricante que permita verificar la funcionalidad ofertada. Cuando el cumplimiento dependa de actividades o servicios a cargo del contratista y no de funcionalidades propias del producto, deberá aportar la evidencia correspondiente mediante metodología, certificación o compromiso formal. La información suministrada deberá ser verificable por la Entidad.**

Firmado digitalmente por wilgenC

WILGEN VICENTE CORREA PADILLA
Subdirector de Servicios de TIC

Aprobado por:	*Wilgen Vicente Correa Padilla*	*27/08/2026*
Proyectado por:	*Jose Huber Otavo - Carlos Hernán Tovar Buitrago*	*27/08/2026*