ANEXO TÉCNICO

1. DENOMINACIÓN DEL BIEN O SERVICIO

OBJETO CONTRACTUAL: Renovar la solución de protección Antivirus de nueva generación para los equipos de cómputo que posee la Secretaría General de la Alcaldía Mayor de Bogotá. D.C.

ALCANCE DEL OBJETO: En el marco de la presente contratación, la Entidad requiere la renovación, configuración, soporte especializado y garantía de la solución Sophos actualmente implementada en la Secretaría General de la Alcaldía Mayor de Bogotá D.C., la cual constituye la plataforma de protección de endpoints y antivirus de nueva generación utilizada para salvaguardar los equipos de cómputo, servidores y demás activos tecnológicos frente a amenazas de seguridad informática.

La contratación contempla no solo la continuidad del licenciamiento y el acceso a las actualizaciones, parches y mejoras liberadas por el fabricante, sino también la prestación de servicios especializados orientados a garantizar la correcta administración, operación, monitoreo y optimización de la plataforma, asegurando el mantenimiento de las condiciones de seguridad, disponibilidad y desempeño requeridas por la Entidad.

Asimismo, se requiere la realización de actividades de configuración avanzada, acompañamiento técnico especializado, y soporte para la implementación y adopción de nuevas funcionalidades incorporadas por el fabricante. En particular, se incluye la habilitación, configuración y puesta en operación de las capacidades de XDR (Detección y Respuesta Extendida), con el propósito de fortalecer las capacidades institucionales de detección, investigación, contención y respuesta ante incidentes de ciberseguridad, permitiendo una gestión más proactiva de las amenazas avanzadas que puedan afectar la infraestructura tecnológica de la Entidad.

De igual manera, el contratista deberá realizar la transferencia de conocimiento al personal designado por la Secretaría General, mediante jornadas de capacitación teórico-prácticas y acompañamiento técnico, orientadas a fortalecer las competencias para la administración de la herramienta, la interpretación de alertas, la gestión de incidentes, la generación de reportes y el aprovechamiento de las funcionalidades avanzadas de la solución, garantizando la apropiación tecnológica y la sostenibilidad operativa de la plataforma durante y después de la ejecución contractual.

Lo anterior contribuirá al fortalecimiento del modelo de seguridad digital de la Entidad, la protección de la información institucional, la reducción de riesgos de ciberseguridad y el cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y de las políticas de seguridad definidas por la Secretaría General de la Alcaldía Mayor de Bogotá D.C. para la protección de sus activos de información.

2. CÓDIGO/S DE LOS SERVICIOS DE ACUERDO CON LA CLASIFICACIÓN UNSPSC

SEGMENTO	FAMILIA	CLASE	PRODUCTO
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43230000 Software	43233200 Software de seguridad y protección	43233205 Software de seguridad de transacciones y de protección contra virus
81000000 Servicios Basados en Ingeniería, Investigación y Tecnología	81110000 Servicios informáticos	81112200 Mantenimiento y soporte de software	81112208 Mantenimiento de software de protección y seguridad

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

Pública

3. CARACTERÍSTICAS Y CONDICIONES TÉCNICAS DE LOS INSUMOS, BIENES, PRODUCTOS, OBRAS O SERVICIOS A ENTREGAR

La Secretaría General de la Alcaldía Mayor de Bogotá gestiona información crítica y confidencial que requiere altos estándares de protección. En el contexto actual de amenazas digitales en constante evolución, las soluciones tradicionales de antivirus ya no son suficientes para hacer frente a ataques sofisticados como ransomware, phishing dirigido (spear phishing), malware polimórfico y amenazas persistentes avanzadas (APT). Por tanto, se hace imperativo implementar una solución de antivirus de última generación (Next-Gen Antivirus – NGAV) que cuente con la funcionalidad de XDR (Detección y Respuesta Extendida) para mejorar la capacidad de detección y respuesta ante amenazas y garantice un entorno digital más seguro y resiliente.

Amenazas emergentes y sofisticadas

La ciberdelincuencia actual emplea técnicas avanzadas que eluden fácilmente las defensas de antivirus convencionales. Los ataques de día cero, los exploits sin archivos (fileless malware) y el ransomware con capacidades de cifrado masivo requieren soluciones que utilicen tecnologías como:

- ✓ Detección basada en comportamiento (behavior-based detection).
- ✓ Inteligencia artificial y aprendizaje automático.
- ✓ Análisis en la nube en tiempo real.
- ✓ Protección contra amenazas sin firmas.

Reducción del riesgo institucional

Una solución NGAV permite detectar y mitigar amenazas en tiempo real antes de que afecten la infraestructura crítica de la Secretaría, minimizando el impacto sobre la continuidad de los servicios, la integridad de la información y la reputación institucional ante la ciudadanía y entes de control.

Cumplimiento normativo

El uso de tecnologías actualizadas para la protección de la información se alinea con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), así como con normas internacionales como la ISO/IEC 27001 y la Ley 1581 de 2012 sobre protección de datos personales. La adquisición de esta tecnología soporta el cumplimiento de los principios de seguridad, disponibilidad y confidencialidad exigidos por la normatividad vigente.

Visibilidad y gestión centralizada

Los NGAV ofrecen plataformas de gestión centralizada con dashboards que permiten monitorear el estado de seguridad de los equipos en tiempo real, generar alertas, reportes automáticos y aplicar políticas homogéneas en toda la red institucional. Esta capacidad es fundamental para la gobernanza de TI en entornos distribuidos como los de la Alcaldía.

Escalabilidad y preparación para el futuro

Una solución moderna permite integrar capacidades de respuesta ante incidentes (XDR), protección frente a amenazas móviles, dispositivos IoT, y expansión hacia arquitecturas híbridas (local y nube), preparando a la entidad para futuras necesidades sin incurrir en nuevos procesos de contratación.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

Pública

Por lo anterior, la Secretaría General de la Alcaldía Mayor de Bogotá D.C. requiere adelantar el proceso de contratación para la renovación, configuración, soporte y garantía de la solución (Sophos) herramienta de protección Antivirus de nueva generación para los equipos de cómputo de la entidad, incluido el módulo XDR (Detección y Respuesta Extendida), que permita realizar como mínimo las siguientes actividades:

- ✓ Monitorear en tiempo real las actividades de los endpoints (dispositivos finales) para detectar comportamientos sospechosos o maliciosos.
- ✓ Generar alertas y realizar análisis detallados de los incidentes de seguridad.
- ✓ Contar con una visión integral de los endpoints en la red para identificar cualquier anomalía o actividad no autorizada en los dispositivos conectados.
- ✓ Detectar y analizar comportamientos inusuales que podrían indicar la presencia de amenazas nuevas o desconocidas. (Inteligencia de amenazas)
- ✓ Mejorar la capacidad de detección y respuesta ante las amenazas identificadas.
- ✓ Apoyar la investigación y análisis de incidentes de seguridad mediante las capacidades disponibles, permitiendo consultar y analizar la telemetría y demás información de seguridad disponible en la plataforma para identificar indicadores de compromiso, actividad sospechosa, activos afectados y demás elementos que contribuyan a determinar el alcance y las posibles causas del incidente.
- ✓ Mitigar vulnerabilidades conocidas, desconocidas y de día cero
- ✓ Identificar ataques post-explotación, es decir acciones maliciosas que ocurren después de que un atacante ha explotado una vulnerabilidad o ha obtenido acceso al sistema.

A continuación, se detallan los requerimientos técnicos con los que cuenta la solución de protección antivirus para los equipos de cómputo de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

Ítem	Descripción
Licenciamiento:	El contratista seleccionado deberá brindar la renovación del licenciamiento y soporte técnico de la solución de protección antivirus para mil trescientos (1300) endpoints (dispositivos finales). Así mismo, debe hacer entrega de la garantía y soporte de la solución de protección antivirus expedida directamente por el fabricante a nombre de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., con vigencia de un (1) año, de acuerdo con lo establecido en el presente Anexo Técnico.
Características Técnicas:	Las características técnicas mínimas que debe cumplir la renovación de la solución de protección antivirus son: • Compatibilidad con los sistemas operativos con los que cuenta la Entidad, como: - Windows 10 y 11 - Windows Server 2019 o versiones posteriores, - MacOS 14 o versiones posteriores - Ubuntu 22.4 o versiones posteriores - Oracle Linux 7 o versiones posteriores • Impacto mínimo en el rendimiento, es decir que sea estable, de tal manera que no afecte ni perjudique el rendimiento de los dispositivos en donde se instale el agente.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

	• Gestión y administración centralizada que permita la configuración de políticas, reglas o tareas específicas para diferentes grupos de usuarios o dispositivos y su replicación automática en los diferentes endpoints (dispositivos finales) en donde se instale el agente. • Contar con una consola de administración centralizada en plataforma cloud, desde la cual se permita gestionar, configurar, monitorear y administrar los componentes y agentes de protección licenciados para la Entidad. • Descarga e instalación automática, centralizada e incremental de todas las actualizaciones, parches y mejoras tecnológicas del software sin costo adicional, tanto para los agentes instalados en cada PC o Servidor, como el software de consola central, incluidas bases de datos de firmas de código malicioso y demás componentes incluidos en la solución de protección antivirus. • Mantener las capacidades disponibles en la solución para la gestión y programación de las actualizaciones de los componentes de protección instalados en los endpoints, de acuerdo con las funcionalidades proporcionadas por el fabricante. • Mantener los mecanismos disponibles en la solución para garantizar la continuidad de las actualizaciones de los componentes y contenidos de protección de los endpoints, permitiendo utilizar las fuentes o mecanismos de actualización disponibles de acuerdo con la arquitectura y funcionalidades proporcionadas por el fabricante. • El motor de exploración deberá utilizar distintas tecnologías de detección virus como, por ejemplo: la exploración de firmas y exploración heurística "busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos", entre otras. • Control y monitoreo del tráfico de red para bloquear accesos no autorizados. • Contar con tecnología XDR (Detección y Respuesta Extendida) para detectar, analizar y responder a amenazas avanzadas en los endpoints (dispositivos finales). • Contar con tecnología que permita la protección en tiempo real mediante el monitoreo constante de archivos y procesos para detectar y prevenir amenazas mientras se ejecutan, así como, el bloqueo de intentos de phishing o sitios web maliciosos, y la prevención y recuperación ante ataques de tipo ransomware (encriptación de archivos). • Escaneo completo del sistema o específicos de discos, carpetas o archivos, donde realice un análisis exhaustivo en busca de amenazas, los cuales puedan desplegarse de manera automática (programados) o manual bajo demanda de los usuarios, a través de la consola de administración o desde la consola y/o agente instalado en el dispositivo final (PC o Servidor). • Mantener las capacidades de protección y análisis de archivos y dispositivos extraíbles disponibles en la solución para detectar, bloquear y prevenir amenazas. Asimismo, mediante las capacidades y/o servicios de inteligencia de amenazas proporcionados por el fabricante, deberá permitir el análisis de archivos sospechosos, incluyendo, cuando se

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

Pública

	encuentre disponible, análisis estático y dinámico en un entorno aislado (sandbox) para determinar su comportamiento, nivel de riesgo e indicadores asociados. • Detección y eliminación de virus, troyanos, exploits, spyware y otro tipo de programa maligno (malware) alojado en múltiples formatos de compresión de archivos como: zip, rar, tar, gzip, entre otros, y la de borrado seguro de este. • Detección y eliminación de comunicaciones a sitios de comando y control con el fin de evitar pérdidas de información, y el bloqueo de scripts maliciosos de Internet Explorer, sean JavaScript o VBScript, entre otros. • Aislamiento de endpoint en caso de malware o comportamientos sospechosos que puedan desencadenar un brote de malware. • Mantener las capacidades disponibles en la solución para la generación y visualización de alertas y notificaciones asociadas a amenazas, detecciones, eventos de seguridad y acciones ejecutadas por los componentes de protección, permitiendo su consulta desde la consola centralizada de administración. • Mecanismos de protección para no permitir la desinstalación o desactivación del agente en los dispositivos y restringir la realización de cambios sobre la configuración de la consola cliente, por parte de los usuarios finales. • Mecanismos de protección que permitan a los administradores de la herramienta habilitar o deshabilitar módulos de protección de manera selectiva, sin necesidad de desinstalarlos del sistema, con el fin de facilitar la solución de conflictos, la realización de pruebas o la aplicación de configuraciones temporales. Estas acciones deberán ser registradas en los logs de auditoría de la consola de administración, identificando el usuario que realizó la modificación, la fecha y hora, y el módulo afectado, garantizando la trazabilidad de los cambios realizados sobre la configuración de seguridad de los endpoints.. • Creación y manejo de listas blancas y negras para prevenir que se ejecuten aplicaciones no autorizadas, permitiendo el bloqueo o filtrado web **o** filtrado de contenido, orientado a la protección basada en perfiles para evitar la conexión a dominios de reputación dudosa o a dominios con contenido maliciosos. • La solución debe estar en capacidad de hacer filtrado web **o** filtrado de contenido orientado a la protección basada en perfiles para evitar la conexión a dominios de reputación dudosa o a dominios reconocidos como fuentes de software y aplicativos maliciosos. • Mantener las capacidades disponibles para la generación, consulta y visualización de informes, reportes, detecciones y alertas relacionadas con la protección de los endpoints, incluyendo información sobre amenazas detectadas y/o bloqueadas, dispositivos afectados, eventos de seguridad, sitios web o categorías web detectadas y demás información disponible de acuerdo con las funcionalidades del licenciamiento. La información deberá poder ser consultada desde la consola centralizada de administración.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

Pública

	• La solución de protección antivirus debe ser instalada y configurada, permitiendo la gestión centralizada y el despliegue masivo del agente o uno a uno en los endpoints (dispositivos finales) que la Entidad determine al momento del despliegue, a través de la consola de administración. El contratista deberá realizar el despliegue del agente en la totalidad de los equipos señalados por la supervisión, garantizando su correcta instalación, configuración y activación de los módulos de protección y XDR. En caso de que se presenten inconvenientes técnicos que impidan el despliegue masivo automatizado, el contratista deberá realizar el despliegue de manera manual o asistida en los equipos que así lo requieran, sin que esto genere costos adicionales para la Entidad ni afecte el plazo de ejecución del contrato. El contratista deberá presentar un informe detallado del despliegue realizado, indicando los equipos intervenidos, las novedades presentadas y las acciones tomadas para su solución. • Mantener las capacidades disponibles en la solución para la detección, remediación y cuarentena de archivos o elementos identificados como maliciosos en los endpoints, de acuerdo con las funcionalidades proporcionadas por el fabricante. • Mantener las capacidades disponibles en la solución para configurar y administrar exclusiones de análisis y protección sobre archivos, carpetas y demás elementos soportados por la plataforma, incluyendo, cuando aplique, la utilización de rutas, nombres de archivo, extensiones y caracteres comodín, de acuerdo con las funcionalidades proporcionadas por el fabricante. • Controlar, gestionar y auditar los dispositivos de almacenamiento externos conectados en los endpoints (dispositivos finales) desde la consola de administración, permitiendo la creación de excepciones por usuario, grupos de usuarios o dispositivos específicos. • Mantener las capacidades disponibles en la solución para la protección de los endpoints frente a intentos de explotación de vulnerabilidades, incluyendo mecanismos de Exploit Mitigation, protección de aplicaciones vulnerables y demás controles de prevención, detección y mitigación de exploits proporcionados por el fabricante. La solución deberá permitir la generación y consulta centralizada de las detecciones, alertas y eventos de seguridad relacionados con estas capacidades desde la consola de administración. • Gestión del inventario de los endpoints (dispositivos finales) y el software instalado en cada dispositivo, con el fin de identificar programas con versiones desactualizadas que puedan comprometer la seguridad. • Permitir la recolección y envío de datos técnicos y de comportamiento desde los endpoints hacia un servidor o consola de administración. (Telemetría), garantizando que dicha funcionalidad se encuentre configurada y operativa, con el fin de facilitar el monitoreo proactivo, la detección temprana de amenazas y la generación de alertas basadas en el análisis de comportamiento de los equipos protegidos. El contratista deberá asegurar que la transmisión de estos datos se realice de manera segura, utilizando protocolos cifrados y cumpliendo con las políticas de protección de datos personales y seguridad de la información de la Entidad.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

Pública

Soporte y garantía:	• Prestar el servicio de acompañamiento y solución de aquellos problemas e incidentes que la consola no resuelve automáticamente, así como, la resolución de dudas y asesoría en mejores prácticas sobre la gestión de la solución de protección antivirus, durante toda la vigencia del soporte y la garantía contratados, en los términos previstos en el numeral de vigencia del presente Anexo Técnico. • Atender los requerimientos de soporte presencial o virtual según solicitud de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., durante el tiempo de soporte. • Proveer el soporte especializado por el término de doce (12) meses, contados a partir de la fecha de activación efectiva de la renovación certificada por el fabricante o su representante autorizado, garantizando la continuidad de la protección sin solución de continuidad respecto de la cobertura actual, sin que se genere cobertura ni cobro retroactivo a cargo de la Entidad por el periodo anterior a la activación. Cuando la activación se produzca en o antes de dicho vencimiento, la vigencia correrá de forma continua hasta el 27 de noviembre de 2027; cuando se produzca con posterioridad, el contratista gestionará ante el fabricante la conservación de la fecha de corte mediante prorrateo o coterminación, sin costo adicional para la Entidad. Así mismo, deberá disponer de diferentes canales de atención (telefónico, correo electrónico, chat, plataforma de gestión, entre otros) para que la Entidad registre los requerimientos y/o incidentes. • Durante la ejecución y el tiempo de garantía, se debe proveer personal certificado en la solución de protección antivirus para la atención de los requerimientos e incidentes reportados por la Entidad. • Suministrar e instalar durante la vigencia del soporte y garantía las actualizaciones estables de software, firmware y parches de la plataforma, en forma integrada, dentro de los siete (7) días hábiles siguientes a la fecha de la liberación por parte del fabricante Sophos, siempre que dichas actualizaciones hayan sido validadas por el fabricante como estables y no presenten conflictos conocidos con la infraestructura tecnológica de la Entidad. El contratista deberá informar previamente a la supervisión del contrato sobre las actualizaciones a aplicar, indicando su alcance, beneficios y eventuales afectaciones, y deberá contar con la autorización expresa de la supervisión para proceder con su instalación en los entornos productivos. • Atender y resolver los requerimientos y/o incidentes reportados por la entidad, sobre la solución de protección antivirus, mediante los canales de atención dispuestos, en un esquema de atención 7x24x365. • El contratista deberá atender los incidentes reportados por la Entidad, clasificándolos de acuerdo con los niveles de severidad establecidos por el fabricante Sophos (Crítico, Alto, Medio, Bajo) . Para la gestión ante el fabricante, el contratista deberá ajustarse a los tiempos de respuesta establecidos por Sophos para cada nivel de severidad: Crítico (4 horas), Alto (8 horas), Medio (24 horas) y Bajo (24 horas) . En caso de que se requiera soporte de tercer nivel (fabricante), el contratista deberá escalar, gestionar y realizar todos los procedimientos que el fabricante solicite, siendo el único responsable de la gestión y seguimiento de los casos ante Sophos, manteniendo informada a la Entidad sobre el estado del ticket.. Para la implementación de los ajustes derivados de estos escalamientos

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

Pública

	que requieran modificaciones o configuraciones sobre la plataforma, deberán realizarse previamente sesiones de trabajo coordinadas con el equipo interno de la Entidad responsable de su administración, con el fin de evaluar, validar y gestionar de manera controlada los cambios requeridos. • El contratista deberá cubrir cualquier faltante de software, licencias complementarias o componentes técnicos necesarios que se requieran para el correcto funcionamiento del servicio adquirido, los cuales no generarán pagos adicionales por ningún concepto ni cancelación de honorarios extras por parte de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., salvo que dichos faltantes correspondan a requerimientos nuevos no contemplados en el alcance del presente Anexo Técnico y que sean solicitados expresamente por la Entidad con posterioridad a la suscripción del contrato.
Documentación:	• Se debe entregar junto con la propuesta la certificación emitida directamente del fabricante de la solución Sophos donde se evidencie que el proponente es distribuidor, partner autorizado o reseller con nivel de membresía mínimo Gold, y que se encuentra autorizado para implementar, configurar y prestar soporte técnico de la solución Sophos, garantizando así la gestión efectiva de la renovación del licenciamiento, el acceso a los canales de soporte oficiales y la correcta actualización de la plataforma. • Entregar la documentación que evidencie la renovación del licenciamiento, garantía y soporte de la solución de antivirus Sophos, la cual deberá ser expedida directamente por el fabricante a nombre de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., con una vigencia de un (1) año, de acuerdo con lo establecido en el presente Anexo técnico. Esta documentación deberá ser entregada a más tardar dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de requerimiento de entrega, y previamente al inicio de la ejecución de las demás actividades del contrato. • Entregar dentro de los 5 días hábiles siguientes a la suscripción del acta de requerimiento de entrega, el protocolo de soporte actualizado, el cual deberá contener como mínimo: i) canales de atención dispuestos (telefónico, correo electrónico, chat, plataforma de gestión de tickets); ii) horarios de atención y disponibilidad; iii) personal asignado al contrato, incluyendo nombres completos, perfiles profesionales, certificaciones vigentes y roles dentro del equipo de trabajo; iv) tiempos de respuesta y solución para cada nivel de severidad, conforme a lo establecido en el presente Anexo Técnico; v) procedimiento para el escalamiento de incidentes ante el fabricante Sophos; vi) procedimiento para la generación y presentación de reportes e informes; y vii) esquema de comunicación y reporte de novedades ante la supervisión del contrato. El protocolo de soporte deberá ser presentado para aprobación de la supervisión, y cualquier modificación posterior deberá ser igualmente aprobada por esta. • Disponer de los manuales y guías para la configuración y uso de la solución de protección antivirus o cualquier otro documento asociado una vez sea activada la licencia y cuando exista una actualización sobre esta. • Suscribir compromiso de confidencialidad con la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

Afinamiento	El proveedor seleccionado deberá realizar el afinamiento de la plataforma de antivirus. La actividad se realizará sobre la última versión actualizada y con personal certificado en la solución de protección antivirus, se entregará un informe, indicando las actividades realizadas y las sugerencias para mantener y mejorar el buen desempeño de la herramienta. **Personalización de políticas de seguridad** Configurar nuevas políticas según perfiles de usuario y niveles de riesgo (por ejemplo: administrativos, técnicos, operativos). Definir nuevas políticas de escaneo en tiempo real, programado y bajo demanda, sin afectar el rendimiento operativo de los equipos. Establecer excepciones seguras solo cuando estén plenamente justificadas (por software legítimo, aplicaciones críticas, etc.). **Activación y configuración de módulos avanzados** Asegurar que estén habilitados los módulos de protección de última generación como: Protección contra ransomware Análisis de comportamiento (heurística avanzada) Detección de amenazas sin archivo (fileless attacks) Firewall local o control de red Prevención de exploits Control de dispositivos externos (USB, almacenamiento, etc.) **Automatización y actualizaciones** Verificar que las actualizaciones se realicen de forma automática y programada, incluso fuera de horarios laborales. Verificar las respuestas automáticas a incidentes comunes (aislamiento del equipo, cuarentena de archivos, bloqueo de procesos). **Registro y auditoría** Verificar si la generación de logs de eventos de seguridad, accesibles y exportables en formatos estándar esta activa Verificar si la configuración de retención de logs en cumplimiento con las políticas de auditoría de la entidad, esta habilitada.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

<table>
<tr><td></td><td>Nota. Por afinamiento se entiende la revisión y ajustes a la configuración del software para optimizar el rendimiento y la configuración de parámetros o políticas que conforman la solución.

Finalmente, el proveedor seleccionado deberá realizar la segunda evaluación (assessment) prevista en las obligaciones específicas, en la que se verifique el afinamiento de la plataforma antivirus. Como resultado, se deberá entregar un informe que indique el estado de funcionamiento de la plataforma, junto con recomendaciones y sugerencias para mantener y mejorar el desempeño de la herramienta.</td></tr>
<tr><td>Transferencias de Conocimiento</td><td>El contratista debe brindar la transferencia de conocimiento acerca del manejo técnico y funcional de las nuevas funcionalidades de la herramienta de protección antivirus e implementación de buenas prácticas, para el aprovechamiento del licenciamiento y del módulo de XDR (Detección y Respuesta Extendida). Dicha transferencia debe contar con una intensidad mínima de (10) horas, para al menos cinco (5) personas, la cantidad de sesiones y horarios serán acordados entre las partes. El contenido de los cursos y el material didáctico debe referirse a la versión más reciente, según currículo oficial del fabricante.

La transferencia de conocimientos debe ser brindada por personal certificado (la certificación del profesional debe estar vigente al momento de realizar la sesión o sesiones de la transferencia de conocimientos). El contratista deberá entregar a la Entidad, una vez finalizada la transferencia, los certificados de participación emitidos a nombre de los asistentes, en los cuales se especifique el contenido, la intensidad horaria y la fecha de realización. Asimismo, deberá entregar el material didáctico utilizado (presentaciones, manuales, guías prácticas y demos) en formato digital, así como los listados de asistencia debidamente firmados por los participantes..

La transferencia de conocimiento deberá ser soportada con el material utilizado (manuales, presentaciones y/o demo) y listados de asistencia.</td></tr>
<tr><td>Equipo de Trabajo:</td><td>El proveedor debe contar con un equipo mínimo de trabajo para la ejecución del contrato, el cual debe estar conformado como mínimo por:

Ingeniero de Implementación:

<table><tr><td>Profesional</td><td>Ingeniería Electrónico o Eléctrico o de sistemas o telecomunicaciones o afines, entendidas como aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional.</td></tr><tr><td>Certificaciones</td><td>Especialista certificado en la solución de protección antivirus Sophos (vigente)</td></tr></table>
Las hojas de vida del personal mínimo, que el proponente seleccionado disponga para la ejecución del contrato deberán ser presentadas dentro de los cinco (5) días calendario siguientes a la firma del contrato.</td></tr>
</table>

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

Pública

4. CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN

Dada la naturaleza de las actividades que se ejecutarán en desarrollo del objeto contractual, el contratista seleccionado deberá garantizar en todo momento la confidencialidad, integridad, disponibilidad y protección de la información institucional a la que tenga acceso, ya sea de manera directa o indirecta, incluyendo aquella suministrada por la Entidad o conocida a través de terceros durante la ejecución del contrato. Para tal efecto, deberá suscribir el correspondiente Compromiso de Confidencialidad y Tratamiento de la Información, el cual hará parte integral del contrato y será de obligatorio cumplimiento durante su ejecución y con posterioridad a su terminación, cuando así lo exijan la naturaleza de la información y la normatividad aplicable.

Así mismo, el contratista será responsable de adoptar las medidas técnicas, administrativas y de seguridad necesarias para garantizar el adecuado manejo, custodia, almacenamiento, acceso y uso de la información entregada o generada con ocasión de la prestación de los servicios de licenciamiento, soporte, mantenimiento y acompañamiento especializado. En consecuencia, se obliga a abstenerse de realizar cualquier acción que pueda comprometer la seguridad de la información, incluyendo, pero sin limitarse a, su reproducción no autorizada, copia, extracción, divulgación, cesión, alteración, eliminación, comercialización o utilización para fines distintos a los previstos en el contrato.

De igual forma, el contratista seleccionado deberá asegurar que su personal, subcontratistas, aliados o terceros vinculados a la ejecución contractual observen los mismos estándares de confidencialidad y seguridad de la información, respondiendo por cualquier incumplimiento que se derive de sus actuaciones. El incumplimiento de estas obligaciones constituirá un incumplimiento contractual y dará lugar a la aplicación de las medidas, sanciones, indemnizaciones y demás acciones a que haya lugar de conformidad con lo establecido en el contrato y en la normativa vigente.

5. NORMATIVIDAD APLICABLE

- La Ley 80 de 1993, Por la cual se expide el Estatuto General de Contratación de la Administración Pública
- Ley 1150 de 2007, por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
- Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1082 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo de Planeación.
- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley número 23 de 1982 y Ley 44 de 1993 – Regulación de protección intelectual
- Resolución 3436 de 2017 del Ministerio de Tecnología de la Información y las Comunicaciones
- Normas que regulan la contratación estatal en Colombia. (Leyes 80 de 1993 y ley 1150 de 2007 y Decreto reglamentarios), el Código Civil y el Código de Comercio Colombiano.
- Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015 – Lineamientos en el manual de Gobierno digital (antes Gobierno en Línea).
- Decreto 410 de 1971 por el cual se expide el código de comercio
- Ley 1480 de 2011 Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones.

6. OBLIGACIONES DEL CONTRATISTA

6.1 Obligaciones Específicas

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

Pública

1. Cumplir integralmente con el objeto contractual, garantizando la ejecución de todas las actividades, productos y servicios requeridos, de conformidad con las condiciones establecidas en el contrato, el Anexo Técnico, la propuesta presentada y los lineamientos impartidos por la supervisión del contrato.
2. Suscribir el Acta de Requerimiento de Entrega dentro de los dos (2) días hábiles siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato
3. Presentar para aprobación de la supervisión, dentro de los cinco (5) días hábiles siguientes a la suscripción del Acta de Requerimiento de Entrega, un cronograma detallado que contemple todas las actividades necesarias para la ejecución del objeto contractual, incluyendo entregables, responsables, hitos, fechas de ejecución y demás aspectos requeridos para el adecuado seguimiento del contrato.
4. Entregar la documentación que acredite la adquisición, renovación y activación de las licencias, así como el soporte y mantenimiento de la solución de protección antivirus, expedida directamente por el fabricante y a nombre de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., garantizando una vigencia mínima de un (1) año de acuerdo con lo establecido en el presente Anexo técnico.
5. Implementar y configurar las funcionalidades de XDR (Detección y Respuesta Extendida) y demás capacidades de seguridad incluidas en el licenciamiento contratado, asegurando su correcta integración con la infraestructura tecnológica de la Entidad y la generación de alertas, monitoreo y capacidades de respuesta ante incidentes de seguridad.
6. Prestar soporte técnico especializado durante la vigencia contractual y de la garantía, atendiendo los requerimientos que formule la Secretaría General de la Alcaldía Mayor de Bogotá D.C., a través del supervisor y/o apoyo a la supervisión del contrato, de conformidad con los niveles de servicio establecidos.
7. Realizar dos (2) evaluaciones de seguridad (assessments) de la solución durante el período de cobertura contratado, conforme a los siguientes hitos: 1. Primer assessments: deberá realizarse dentro de los treinta (30) días calendario siguientes a la suscripción del acta de requerimiento de entrega, como diagnóstico inicial de la solución e insumo para las actividades de afinamiento de la plataforma. 2. Segundo assessments: deberá realizarse al cumplirse seis (6) meses contados desde el inicio de la cobertura de la garantía y soporte, con el propósito de verificar la implementación y efectividad de los ajustes efectuados, el tratamiento de los hallazgos derivados de la primera evaluación y el estado de seguridad de la solución. Cada evaluación deberá comprender, como mínimo, la revisión del estado de la solución; la identificación, análisis y valoración de los hallazgos disponibles en la plataforma Sophos; la revisión de las configuraciones de seguridad; el análisis de la efectividad de las políticas implementadas; y la formulación de recomendaciones orientadas al fortalecimiento de la postura de ciberseguridad de la Entidad. Como resultado de cada assessments, el contratista deberá presentar un informe técnico detallado, que contengan como mínimo: i) metodología utilizada; ii) hallazgos identificados; iii) nivel de criticidad de cada hallazgo; iv) recomendaciones específicas para su tratamiento o corrección; y v) plan de acción sugerido, incluyendo los plazos estimados para su implementación. Para la segunda evaluación, el informe deberá incorporar los hallazgos evidenciados y las recomendaciones. Los informes deberán ser entregados a la supervisión del contrato dentro de los cinco (5) días hábiles siguientes a la finalización de cada assessments.
8. Gestionar oportunamente las actualizaciones, parches, correcciones y mejoras liberadas por el fabricante, garantizando que la solución permanezca soportada, actualizada y alineada con las mejores prácticas de seguridad y operación.
9. Realizar la transferencia de conocimiento, de conformidad con lo establecido en el Anexo Técnico, mediante sesiones teórico-prácticas dirigidas al personal designado por la Entidad, incluyendo la administración de la solución, gestión de incidentes, operación de las funcionalidades XDR, generación de reportes y mejores prácticas de seguridad.
10. Cumplir con la Política de Seguridad Digital, la Política de Tratamiento de Datos Personales, el Sistema de Gestión de Seguridad de la Información (SGSI) y demás lineamientos de seguridad de la información

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

Pública

establecidos por la Secretaría General de la Alcaldía Mayor de Bogotá D.C., garantizando la confidencialidad, integridad, disponibilidad y protección de la información institucional a la que tenga acceso. Para tal efecto, el contratista deberá suscribir el compromiso de confidencialidad y tratamiento de datos personales que la Entidad establezca, y deberá asegurar que todo su personal, subcontratistas y tercero s vinculados a la ejecución del contrato observen los mismos estándares de seguridad. El incumplimiento de estas obligaciones dará lugar a las acciones legales y contractuales correspondientes.

11. Obligaciones específicas en materia de tratamiento y protección de datos: Para efectos de esta sección, la Secretaría General de la Alcaldía Mayor de Bogotá D.C. actúa como Responsable del Tratamiento y EL CONTRATISTA como Encargado del Tratamiento, respecto de los datos personales contenidos en la telemetría, registros (logs), alertas, detecciones, archivos en cuarentena y demás información a la que acceda con ocasión de la operación de la solución antivirus/XDR (Ley 1581 de 2012). En tal calidad, EL CONTRATISTA asume las siguientes obligaciones:

a) Tratar la información y los datos personales a los que acceda con ocasión del contrato únicamente por cuenta y bajo las instrucciones de la Entidad, con la finalidad exclusiva de prestar los servicios de protección, detección y respuesta contratados, conforme a la Ley 1581 de 2012, el Decreto 1074 de 2015, el Modelo de Seguridad y Privacidad de la Información (MSPI) y las políticas de seguridad y de tratamiento de datos de la Secretaría General.

b) Abstenerse de usar, reproducir, extraer, copiar, transferir, comercializar o divulgar la telemetría, los registros, las detecciones o cualquier información de la Entidad para fines distintos de la ejecución del contrato, propios o de terceros. En particular, no podrá utilizar dicha información para entrenar o alimentar modelos, productos o servicios propios sin autorización previa, expresa y escrita de la Entidad.

c) Acceder a la consola, los endpoints y la información bajo el principio de mínimo privilegio, limitando el acceso a lo estrictamente necesario para la prestación del servicio, y llevar registro de los accesos y de las actividades que realice, disponible para la supervisión cuando le sea requerido.

d) Implementar y mantener medidas técnicas, humanas y administrativas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información a la que acceda, e impidan su acceso no autorizado, alteración, pérdida o divulgación indebidos.

e) Guardar reserva y confidencialidad sobre toda la información conocida con ocasión del contrato, deber que subsiste de manera indefinida con posterioridad a la terminación y liquidación del contrato, y hacerlo extensivo a su personal mediante los acuerdos de confidencialidad que la supervisión requiera.

f) No transferir ni transmitir la información a terceros ni subcontratar su tratamiento sin autorización previa, expresa y escrita de la Entidad; cuando se autorice, trasladará al tercero las mismas obligaciones de seguridad, finalidad y confidencialidad aquí previstas, permaneciendo responsable ante la Entidad.

g) Informar a la supervisión, sin dilación indebida y a más tardar dentro de las cuarenta y ocho (48) horas siguientes a su conocimiento, cualquier incidente de seguridad, acceso no autorizado o violación de datos personales que afecte la información de la Entidad, indicando su alcance y las medidas adoptadas.

A la terminación del contrato, o en cualquier momento a solicitud de la Entidad, devolver la información de la Entidad a la que haya accedido y suprimir de forma segura y definitiva las copias, extracciones o registros que conserve en sus sistemas o los de sus proveedores autorizados, salvo deber legal de conservación, sobre el cual mantendrá las obligaciones de seguridad y confidencialidad aquí previstas. La supresión se certificará por escrito ante la supervisión.

12. Las demás obligaciones inherentes a la naturaleza del contrato y aquellas que resulten necesarias para garantizar la correcta, oportuna y eficiente ejecución del objeto contractual, de conformidad con las disposiciones legales vigentes y los documentos que integran el proceso de selección y el contrato.

7. PLAZO DE EJECUCIÓN

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

Pública

El plazo para la ejecución del contrato será de CUARENTA (40) DÍAS CALENDARIO sin exceder el 31 de diciembre de 2026, contados a partir de la fecha de suscripción del acta de requerimiento de entrega, previo cumplimiento de los requisitos de perfeccionamiento y ejecución.

PARÁGRAFO PRIMERO. El contratista deberá acreditar la entrega y activación de la renovación de las licencias dentro de los cinco (5) días Hábiles siguientes al acta de requerimiento de entrega.

PARÁGRAFO SEGUNDO. Sin perjuicio del vencimiento del plazo de ejecución contractual (40 días), el contratista garantiza que el servicio de licenciamiento, soporte técnico especializado y actualizaciones (como obligaciones integrantes de la Garantía Técnica de Calidad y Funcionamiento del bien), cubrirán de forma ininterrumpida, asegurando la garantía y soporte hasta el 27 de noviembre de 2027.

8. LUGAR DE EJECUCIÓN

El sitio de ejecución del presente contrato se realizará en las sedes de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

9. FORMA DE PAGO DEL VALOR DEL CONTRATO

La Secretaría General de la Alcaldía Mayor de Bogotá D.C realizará el pago, así:

Un único pago correspondiente al valor del contrato por la renovación del licenciamiento del Antivirus Sophos, el cual se efectuará una vez se verifique el cumplimiento de las siguientes condiciones:

- La presentación del documento expedido por el fabricante o su representante autorizado, en el que se evidencie la renovación del soporte y mantenimiento adquiridos, así como la vigencia correspondiente del licenciamiento.
- La entrega de los documentos y soportes que acrediten la ejecución de las actividades contractuales asociadas a la renovación.
- La realización y acreditación de la transferencia de conocimiento prevista en el contrato, incluyendo las memorias, registros o evidencias correspondientes.
- La suscripción del recibo a satisfacción por parte del supervisor del contrato, previa validación del cumplimiento integral de las obligaciones a cargo del contratista.

El pago se realizará de conformidad con los procedimientos financieros establecidos por la Entidad y estará sujeto a la acreditación del cumplimiento de los requisitos contractuales, legales y tributarios aplicable.

El pago se realizará previa presentación de los siguientes documentos:

- Informe de actividades adelantadas durante el periodo, aprobado por el apoyo a la supervisión del contrato.
- Certificado de cumplimiento de obligaciones Expedida por la Supervisión del contrato
- Acta de recibo a satisfacción expedido por el supervisor del contrato.
- Factura
- Certificación suscrita por el representante legal o revisor fiscal (cuando aplique), que acredite el cumplimiento del pago de aportes al sistema de seguridad social integral, parafiscales, ICBF, SENA y cajas de compensación familiar de los últimos seis (6) meses, de conformidad con el artículo 50 de la Ley 789 de 2002 o aquella que lo modifique, adicione o complemente, cuando se trate de personas jurídicas

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

Pública

Los pagos se efectuarán previa verificación del cumplimiento de los requerimientos y condiciones técnicas solicitadas en la ficha técnica y demás documentos que formen parte integral del/los contrato/s.

NOTA 1: Dichas sumas se pagarán dentro de los treinta (30) días calendario siguientes a la presentación y radicación de la factura por parte del contratista, la certificación de cumplimiento de compromisos contractuales por parte del supervisor y la certificación del revisor fiscal o representante legal, según corresponda, sobre el cumplimiento en el pago de los aportes parafiscales y de seguridad social integral de sus empleados de acuerdo con lo establecido en el artículo 50 de la ley 789 de 2002 y articulo 23 de la ley 1150 de 2007, y demás normas que regulan la materia.

NOTA 2: LA SECRETARÍA GENERAL sólo adquiere obligaciones con quien resulte contratista del presente proceso y bajo ningún motivo o circunstancia efectuará pagos a terceros.

NOTA 3: El pago será realizado por medio de la Tesorería Distrital en pesos colombianos, a través de la consignación en la cuenta corriente o de ahorros que indique el contratista, abierta en una de las entidades financieras afiliadas al Sistema Automático de pagos, previos los descuentos de Ley.

NOTA 4: Dentro del término señalado para efectuar el pago, **LA SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C.** podrá formular por escrito las observaciones u objeciones que tenga a la factura, que presente para el pago EL CONTRATISTA. Durante el tiempo que dure la revisión a las observaciones formuladas por **LA SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C.**, se suspenderá el plazo para el pago y una vez realizadas las aclaraciones pertinentes por parte del CONTRATISTA se reanudará dicho plazo.

NOTA 5: El CONTRATISTA con la suscripción del contrato, acepta que en el evento que el valor total a pagar por cada factura tenga centavos, estos se ajusten o aproximen al peso, ya sea por exceso o por defecto, si la suma es mayor o igual a 0.50 se ajustara por encima, del contrario se ajustará hacia abajo. Lo anterior, sin que sobrepase el valor total establecido en el contrato.

NOTA 6: Todos los pagos se realizarán conforme a la programación y disponibilidad del PAC de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. previa aprobación del PAC (Programa Anual Mensualizado de Caja).

ARLETH PATRICIA SAURITH CONTRERAS
Jefe Oficina de Tecnologías de la Información y las Comunicaciones
Oficina de Tecnologías de la Información y las Comunicaciones

Elaboró: Lourdes María Acuña Acuña / Erika Tatiana Quintero Quintero – Contratistas OTIC
Revisó: Sandra Viviana Muñoz – Contratista OTIC
Reviso: Jorge Porras – Contratista Oficina Consejería Distrital de TIC

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195