Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

ESPECIFICACIONES TÉCNICAS

SELECCIÓN ABREVIADA POR SUBASTA INVERSA

ESTUDIO PREVIO 41462 DE 2026

OBJETO

Suscripción al soporte y actualización del sistema de filtrado de contenido web SWG.

ALCANCE DEL OBJETO

Por medio de este proceso de contratación se pretende contratar la suscripción al soporte y actualización de un sistema de Filtrado de Contenido Web SWG por un año, de acuerdo con los Acuerdos de Niveles de Servicio (ANS) establecidos en las especificaciones técnicas; lo anterior para la correcta operación de este sistema, el cual mitiga los riesgos al navegar en Internet.

OBJETIVO GENERAL

Mitigar los riesgos a los que está expuesta la información, por medio de la adquisición al soporte y actualización de un dispositivo de filtrado, monitoreo de contenido web, el cual por medio de controles tecnológicos inspecciona la navegación a internet de todos los usuarios y el bloqueo de páginas que pueden generar un riesgo para los datos personales de los usuarios, con los cuales se brinda la atención a la ciudadanía.

De esta manera se reduce la probabilidad de fallas de disponibilidad, confidencialidad e integridad de la información, aumentando la confianza de los visitantes y/o ciudadanía en general y otorgando cumplimiento con lo reglamentado en la ley 1581 de 2012 *"por la cual se dictan disposiciones generales para la protección de datos personales"*, en su *"Art 18 Literal b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"*.

OBJETIVOS ESPECÍFICOS

- Disminuir al máximo las vulnerabilidades a la que se expone la información, por medio de la suscripción al soporte y actualización de un sistema de Filtrado de Contenido Web SWG.
- Aumentar la confianza de los funcionarios al utilizar sitios web, ya que se tendría un dispositivo de filtrado, monitoreo de contenido web que brinda protección a los portales que se ingresan.
- Ofrecer integridad de la información, por medio de la suscripción al soporte y actualización de un sistema de Filtrado de Contenido Web SWG.

ESPECIFICACIONES TÉCNICAS.

El proponente deberá garantizar las siguientes especificaciones:

1. HARDWARE

- Actualmente se cuenta con una plataforma de Filtrado de Contenido Web Skyhigh Web Gateway (SWG), compuesta por dos (2) Appliances de las referencias WG 5500E y WG 5500F, de los cuales se reemplazará uno (1), correspondiente al modelo WG 5500E, por un nuevo Appliance de la referencia WG 5500F.

- El Appliance de referencia WG 5500E actualmente cuenta con garantía; no obstante, este dispositivo deberá ser reemplazado por un nuevo dispositivo de la referencia WG 5500F, el cual deberá contar con una garantía de doce (12) meses a partir de su instalación y puesta en producción.

- El Appliance de referencia WG 5500F cuenta con garantía hasta el 13 de julio de 2026. Este dispositivo no será reemplazado; sin embargo, su garantía deberá ser renovada por un período de doce (12) meses, contados a partir de la suscripción del contrato.

2. SOFTWARE Y LICENCIAMIENTO

Actualmente, se cuenta con el siguiente licenciamiento:

- Licencias: 7001 usuarios nombrados de Skyhigh SWG Anti-Malware AddOn.
- Licencias: 7001 usuarios nombrados de Skyhigh SWG Software – Suscripción.
- Licencias: 3001 usuarios de Skyhigh SWG Cloud Services.
- Licencias: 3001 usuarios de Trellix ePO-SaaS for SSE – AddOn.
- El licenciamiento solicitado deberá renovarse por un período de doce (12) meses; no obstante, dos mil un (2001) licencias de Skyhigh SWG y dos mil un (2001) licencias de Trellix ePO-SaaS for SSE – AddOn deberán renovarse por un período de ocho (8) meses.
- La consola Trellix ePO-SaaS for SSE – AddOn deberá contar con la capacidad de administrar las 3001 licencias de Skyhigh SWG Cloud Services.
- El sistema operativo de los Appliances deberá ser Linux endurecido o propio del fabricante.
- Las licencias de los equipos, software de servidor y clientes deberán proveerse a perpetuidad, sin costo de licenciamiento adicional. Lo anterior implica que la solución no deberá dejar de operar en caso de no renovación del contrato de soporte; sin embargo, los módulos de actualización (tales como nuevas categorías de filtrado, listas negras, nuevas versiones de firmware y actualizaciones de malware) podrían no estar disponibles.
- El licenciamiento deberá contemplar la totalidad de los componentes requeridos, incluyendo servidores, hosts y demás elementos que hagan parte de la solución, así como los productos complementarios de su familia tecnológica.
- No se aceptará la instalación de software cliente en estaciones de trabajo, salvo en aquellos equipos que no se encuentren en la red corporativa o que estén ubicados en

sedes externas del Distrito, para los cuales aplique la instalación del cliente Skyhigh® Web Gateway Cloud Service.

3. SOPORTE.

- El servicio de soporte deberá ser prestado por personal certificado en la solución.
- Se deberá garantizar el soporte por un período de doce (12) meses para la atención integral de la Plataforma de Filtrado de Contenido Web.
- El contratista, durante la atención de los casos de soporte, deberá reportar tanto el número de los casos asignados por él como el número de casos generados ante el fabricante.
- Los requerimientos (casos de soporte o tickets) no podrán ser cerrados sin la autorización previa del supervisor del contrato.
- Se deberán realizar las visitas que sean necesarias para la solución de incidentes.
- El contratista deberá garantizar que los hallazgos o mejoras detectados en la herramienta, que deban ser escalados al fabricante por dificultades en el servicio, sean gestionados y solucionados conforme a los Acuerdos de Niveles de Servicio (ANS).
- El contratista deberá garantizar que, en caso de que el fabricante requiera escalar una falla a su área de desarrollo, el tiempo empleado en su solución sea compensado mediante la ampliación equivalente en la vigencia de las licencias y del soporte.
- Las actividades de actualización deberán programarse en horarios previamente autorizados por el Distrito de Medellín (horarios no laborales) y serán ejecutadas por el contratista, quien deberá entregar el respectivo plan de trabajo.
- El servicio en línea de desbloqueo deberá prestarse sin costo adicional.
- El servicio de soporte para los incidentes reportados deberá atenderse de conformidad con los ANS establecidos.
- El proponente deberá garantizar que la atención por parte del fabricante, a través de los canales telefónico, correo electrónico, soporte remoto y/o chat, se preste con disponibilidad 5x8 (de lunes a viernes, de 8:00 a. m. a 12:00 m y de 1:00 p. m. a 5:00 p. m.), durante la vigencia del contrato.
- Se deberá garantizar acompañamiento en actualizaciones y/o mejoras previamente acordadas, en horarios diferentes a la atención 5x8, sin costo adicional para el Distrito de Medellín, teniendo en cuenta que dichas actividades no podrán realizarse en horario laboral.
- Las actualizaciones de firmware realizadas por el fabricante durante el período del contrato deberán estar incluidas dentro del presupuesto, y el contratista deberá apoyar su instalación y puesta en funcionamiento.

4. ESPECIFICACIONES PLATAFORMA.

4.1 El proponente deberá garantizar y conservar las siguientes características:

- El producto no deberá encontrarse en estado de End of Sale durante los próximos tres (3) años.
- La plataforma deberá ser compatible con direccionamiento IP versión 6 (IPv6).
- La solución deberá ser compatible con sistemas operativos Windows (7, 8, 8.1, 10 y 11), así como con Windows Server (2003, 2008, 2008 R2, 2012, 2016, 2019, 2022 y 2025), en arquitecturas de 32 y 64 bits, y con sistemas Linux en arquitecturas de 32 y 64 bits.

- La solución deberá integrarse con servicios LDAP basados en roles, incluyendo la compatibilidad con servidores como OpenLDAP, Lotus Domino, iPlanet LDAP y Microsoft Active Directory.
- La solución deberá permitir la integración con Microsoft Active Directory sin requerir la instalación de componentes adicionales en los controladores de dominio. Esta integración deberá permitir la administración de la solución mediante cuentas de usuario y grupos definidos en el Active Directory.
- Administración basada en roles: la solución deberá permitir la segregación de funciones de manera granular, diferenciando claramente los roles de seguridad de sistemas y otras unidades definidas en el Active Directory, así como el alcance y las capacidades de gestión de cada administrador.
- Los componentes de software, así como sus respectivas actualizaciones, deberán ser compatibles con el hardware y software existente en el Distrito de Medellín; en caso contrario, el proveedor deberá asumir el suministro e implementación del hardware adicional requerido, sin costo para la entidad.
- La solución deberá permitir la personalización de la configuración, de acuerdo con las necesidades de la entidad.
- La solución deberá permitir su administración a través de interfaces gráficas (GUI) y de línea de comandos (CLI).
- La solución deberá permitir el monitoreo en tiempo real de la navegación.
- La solución deberá permitir la integración con sistemas de almacenamiento SAN, NAS o servidores de archivos, para el almacenamiento y gestión de históricos de reportes.
- La solución deberá soportar autenticación mediante Kerberos y NTLM.
- La solución deberá permitir el envío de registros (logs) mediante protocolo syslog hacia un SIEM u otra herramienta que procese tramas equivalentes a syslog.
- La solución deberá permitir la generación de respaldos y la restauración de configuraciones.
- La solución deberá permitir la presentación de páginas web informativas al usuario final, con mensajes configurables por los administradores del sistema, en caso de incidencias o incumplimiento de políticas.
- Las políticas, paneles de control, informes y demás funcionalidades deberán estar disponibles a través de una consola o interfaz gráfica, con el fin de optimizar los tiempos de administración y facilitar su operación.
- La solución deberá ser compatible con los principales navegadores de internet, incluyendo Internet Explorer 10 o superior, Google Chrome, Mozilla Firefox, Opera, Microsoft Edge y Safari.

4.2 Políticas de filtrado de contenido:

- La solución deberá contar con la capacidad de utilizar expresiones regulares para la creación de políticas.
- La solución deberá contar con la capacidad de utilizar expresiones booleanas para la creación de políticas.
- La solución deberá permitir la definición de políticas en forma anidada o encadenada.
- La solución deberá operar como Web Proxy en modo explícito y transparente, con soporte para múltiples mecanismos de autenticación.

- La solución deberá permitir la inspección de tráfico HTTPS mediante la ruptura de certificados SSL.
- La solución deberá disponer de listas negras y listas blancas de sitios web, con actualización automática y la posibilidad de configuración manual por parte del administrador.
- La solución deberá contar con un motor de análisis de contenido que permita determinar, mediante la asociación de palabras clave, si el contenido debe ser permitido o bloqueado.
- La solución deberá permitir la detección y gestión de palabras clave prohibidas, incluyendo acciones como el reemplazo por caracteres de sustitución, el bloqueo de la página o la identificación y bloqueo mediante URL.
- La solución deberá permitir la priorización de políticas de filtrado en función de su criticidad para la entidad.
- La solución deberá permitir el monitoreo de puertos, así como el control de aplicaciones y protocolos.
- La solución deberá contar con al menos setenta (70) categorías predefinidas de filtrado.
- La solución deberá permitir la configuración de categorías personalizadas.
- La solución deberá permitir habilitar o restringir la carga (upload) de archivos en la web.
- La solución deberá permitir habilitar o restringir la descarga de archivos desde la web.
- La solución deberá permitir el bloqueo de contenido de tipo Streaming Media.
- La solución deberá permitir un filtrado granular de redes sociales (como Facebook, Instagram, Twitter, Pinterest, Google+ y similares), incluyendo el control de acciones tales como chatear, publicar, ejecutar aplicaciones, compartir y subir archivos o contenido.
- La solución deberá permitir el control del tráfico tipo Peer-to-Peer (P2P) y de los protocolos asociados.
- La solución deberá permitir el filtrado de tráfico no HTTP, incluyendo aplicaciones P2P (como eMule) y mensajería instantánea (IM).
- La solución deberá permitir el control de acceso a aplicaciones de mensajería y comunicación, tales como WhatsApp Business, Telegram Business, Facebook Messenger, WeChat y Slack o similares.
- La solución deberá aplicar funciones de filtrado de contenido a diferentes protocolos y aplicaciones, tales como chat, foros, telefonía en línea, plataformas P2P y mensajería instantánea.
- La solución deberá permitir la inspección del tráfico de entrada y salida en protocolos HTTP, HTTPS, FTPS y FTP.
- La solución deberá contar con capacidad de almacenamiento en caché (cache) de páginas web.
- La solución deberá permitir la navegación funcional sobre servicios FTP, incluyendo la visualización de estructuras, fechas de modificación y contenido disponible en los directorios habilitados.
- La aplicación de las políticas deberá realizarse en tiempo real, sin requerir que el usuario cierre o reinicie su navegador.
- La solución deberá permitir la ruptura de certificados SSL para el filtrado de sitios que utilizan protocolo HTTPS.

4.3 Políticas de tiempo por usuario, grupos de usuarios, archivos o url para el filtrado de contenido:

- Las políticas de acceso deberán basarse en parámetros como dirección IP, rangos de direcciones IP, subredes y CIDR, así como en usuarios, grupos de usuarios y unidades organizativas (OU) del Active Directory, y segmentos de red.
- Las políticas de filtrado deberán permitir la visualización de videos o grupos de videos (canales), aun cuando la categoría correspondiente se encuentre bloqueada.
- Las políticas de filtrado deberán poder aplicarse en función de la dirección IP, nombre de máquina (registrado en DNS) o usuario del Active Directory.
- La solución deberá permitir la definición de un número ilimitado de perfiles, los cuales podrán combinar parámetros de filtrado como horarios, tipos de archivo, listas personalizadas, desbloqueos, duración de acceso y capacidad de consumo en megabytes (MB).
- La solución deberá permitir el filtrado por usuario o grupo de usuarios, con base en la capacidad de consumo de un sitio web específico o de una categoría.
- La solución deberá permitir el filtrado por usuario o grupo de usuarios, con base en el tiempo de consumo de un sitio web específico o de una categoría.
- La solución deberá permitir el control de cuotas para los usuarios en función del tiempo consumido.
- La solución deberá permitir el control de cuotas para los usuarios en función de la cantidad de datos consumidos, medidos en bytes, durante un período determinado.
- La solución deberá soportar la configuración de tiempos de conexión mediante la definición de reglas específicas.
- La solución deberá permitir el control de límites de tiempo, con múltiples opciones de autenticación aplicables a usuarios y grupos.
- La solución deberá contar con capacidades de filtrado basadas en criterios como reputación de archivos, tamaño del archivo, extensión, encabezados, y el usuario o grupo que realiza la descarga.
- La solución deberá permitir el filtrado de acceso a nivel de subdominios de una URL.
- La solución deberá permitir el filtrado de acceso a nivel de directorios dentro de una URL.

4.4 Protección antimalware:

- La solución deberá contar con capacidades de protección contra phishing y suplantación de sitios web.
- La solución deberá permitir la protección de los usuarios frente a amenazas como virus, spyware, troyanos, scam, malware, phishing, botnets y gusanos que puedan afectar los equipos de cómputo.
- La solución deberá permitir la evaluación en tiempo real de contenidos, scripts y otros componentes potencialmente maliciosos.
- La solución deberá contar con al menos dos (2) motores antimalware integrados.
- La solución deberá permitir la detección de malware tanto entrante como saliente de la red.
- Las firmas de seguridad deberán actualizarse de forma automática, así como bajo demanda por parte de los administradores.
- La solución deberá permitir la detección heurística proactiva de amenazas.

4.5 Actualizaciones:

- La solución deberá contar con actualizaciones automáticas en tiempo real de listas y parámetros, mediante el uso de paquetes incrementales continuos.
- La solución deberá recibir actualizaciones inmediatas frente a nuevas amenazas durante todo el período contractual.
- La solución deberá permitir la migración a nuevas versiones estables de la herramienta.
- Las actualizaciones de firmware y las migraciones a nuevas versiones requeridas deberán ser informadas oportunamente. La instalación de estas deberá ser realizada por el contratista y el fabricante, bajo su responsabilidad, durante la vigencia del contrato, y deberá estar incluida dentro del presupuesto.
- Las actualizaciones de los filtros por reputación de URL deberán realizarse en tiempo real, de manera continua, una vez sean identificadas y liberadas por el fabricante.
- La plataforma deberá mantenerse en la última versión estable disponible durante la ejecución del contrato.

Notas:

Todos los trabajos de actualización de firmware deberán ser oportunamente notificados, debidamente documentados y contar con el respectivo acompañamiento por parte del contratista.

Las nuevas funcionalidades integradas en las actualizaciones deberán ser notificadas y documentadas al supervisor del contrato de manera oportuna.

4.6 Reportes:

- El módulo de reportes deberá estar incluido en la solución, sin costo adicional.
- La plataforma deberá permitir identificar si una política está siendo utilizada, reportando la cantidad de coincidencias en un período de tiempo determinado, por usuario o por grupo.
- La solución deberá contar con reportes predefinidos.
- La solución deberá permitir la generación de informes dinámicos con periodicidad diaria, semanal y mensual, con disponibilidad de datos en archivos planos y la opción de envío automático de reportes.
- La solución deberá permitir consultar la política asociada a un grupo, dirección IP o usuario específico.
- La solución deberá permitir la exportación de las políticas implementadas mediante reportes en formatos como Excel, PDF, CSV y TXT, teniendo en cuenta su prioridad de aplicación.
- La solución deberá permitir la exportación de informes, incluso aquellos que superen los cinco mil (5.000) registros, a formatos como PDF, TXT, CSV u otros equivalentes.
- La solución deberá permitir la importación de listas de acceso, políticas y mapeos.
- La solución deberá permitir la generación de informes orientados a la detección de malware.
- La solución deberá generar reportes del uso de ancho de banda por usuario o por grupo.
- La solución deberá permitir la generación de reportes históricos.

- La solución deberá permitir la generación de reportes de actividad de los usuarios.
- La solución deberá permitir la generación de reportes de sitios bloqueados.
- La solución deberá permitir la programación y envío automático de reportes por correo electrónico.
- La solución deberá proporcionar información para análisis forense, incluyendo datos de quién, qué, cuándo, dónde y cómo, asociados a incidentes de seguridad.
- La solución deberá permitir la visualización en tiempo real del comportamiento del procesador, memoria y capacidad del equipo.

5. INSTALACIONES O CONFIGURACIONES.

- La instalación o configuración de la solución que involucre los equipos tipo Appliance (hardware), en caso de requerirse (por ejemplo, por reposición en garantía), deberá realizarse en sitio por personal certificado en la solución.
- La instalación o configuración de los agentes de licenciamiento (software) deberá ser realizada por personal certificado en la solución.
- La solución deberá integrarse con la infraestructura tecnológica existente del Distrito de Medellín.
- El contratista deberá realizar y verificar las pruebas de integración de la solución.
- La solución deberá permitir una arquitectura centralizada, en la que la instalación principal se realice en un equipo servidor que actúe como nodo principal, a través del cual se gestione y filtre el tráfico de los demás equipos de la red, sin requerir la instalación del software en todas las estaciones de trabajo.
- La solución deberá permitir la ruptura de certificados SSL para el filtrado de sitios que utilizan protocolo HTTPS, con una capacidad mínima de cinco (5) instancias o configuraciones simultáneas.

Nota:

Todas las actividades descritas anteriormente deberán realizarse en las instalaciones del Distrito de Medellín, sin costo adicional para la entidad.

En caso de presentarse fallas en la solución o herramienta, el contratista deberá garantizar la atención en sitio de manera continua, hasta lograr una solución definitiva, confiable y estable.

6. GARANTÍA DE LA SOLUCIÓN.

- La garantía requerida por el Distrito de Medellín a nivel de hardware corresponde a los dos (2) Appliances de referencia WG 5500F, deberá ser por doce (12) meses, contados a partir de la fecha de inicio de ejecución de esta vigencia.
- Con respecto a la garantía del software Skyhigh SWG y Trellix ePO-SaaS for SSE - AddOn Cloud, esta deberá ser por períodos de doce (12) meses y ocho (8) meses, según aplique al licenciamiento, contados a partir de la fecha de recibo a satisfacción, puesta en operación o último vencimiento, según corresponda.
- En caso de requerirse reemplazo de equipos, el envío deberá efectuarse de manera inmediata a la notificación por parte del Distrito de Medellín, y todos los costos asociados

(incluyendo transporte, nacionalización y demás gastos) deberán ser asumidos por el contratista.
- La solución deberá permitir la migración a nuevas versiones sin afectar la continuidad del servicio.
- La solución deberá permitir la implementación de servidores virtuales como mecanismo de contingencia, sin requerir costos adicionales de licenciamiento, en caso de presentarse fallas que afecten la prestación del servicio.
- En caso de que se detecten fallas en el hardware de la solución, el contratista deberá asumir en su totalidad los costos asociados a su reparación, reemplazo o actualización (incluyendo, entre otros, memoria, procesador, discos duros u otros componentes).

7. CANALES PARA EL SOPORTE TÉCNICO REQUERIDO POR EL DISTRITO DE MEDELLÍN (MEDIOS DE COMUNICACIÓN).

- **Soporte por correo electrónico**: La atención se deberá prestar a través de un buzón de soporte previamente informado, y deberá gestionarse de acuerdo con la criticidad del incidente. En caso de modificación del buzón, el contratista deberá informar dicho cambio de manera anticipada.

- **Soporte telefónico**: La atención deberá prestarse a través de los números telefónicos previamente suministrados, conforme a la criticidad del incidente. Cualquier cambio en los números de contacto deberá ser informado con antelación por el contratista.

- **Soporte remoto**: El acceso remoto a los equipos deberá contar con la autorización previa del Distrito de Medellín, con el fin de garantizar la seguridad y el control en el acceso.

- **Soporte por chat**: La atención mediante chat deberá prestarse de acuerdo con la criticidad del incidente. En caso de modificación del canal de atención, el contratista deberá informar dicho cambio de manera anticipada.

8. ENTREGABLES.

- El contratista deberá entregar certificación de garantía por doce (12) meses para el hardware, así como certificación de garantía de doce (12) y ocho (8) meses para el software, según aplique al licenciamiento. Estas deberán contarse a partir de su vencimiento y entregarse en un plazo máximo de ocho (8) días calendario desde el inicio de la ejecución del contrato, autorizado por el supervisor a través de la plataforma SECOP II.
- El contratista deberá entregar los manuales y la documentación actualizada de la última versión de la solución, incluyendo administración, configuración, parametrización e instalación, aplicables al Distrito de Medellín. Este entregable deberá presentarse en un plazo máximo de ocho (8) días calendario a partir del inicio de la ejecución del contrato.
- El contratista deberá entregar un plan de contingencia de la plataforma en un plazo máximo de un (1) mes calendario, contado a partir del inicio de la ejecución del contrato.
- El contratista deberá suministrar los datos de contacto para soporte, junto con un instructivo para la generación de casos. Este entregable deberá presentarse en un plazo

máximo de ocho (8) días calendario a partir del inicio de la ejecución del contrato. En caso de modificación de los canales de soporte, este documento deberá ser actualizado de manera inmediata.

- El contratista deberá entregar el plan de trabajo y la metodología de implementación de la solución, incluyendo el reporte de las actividades a desarrollar, a partir del inicio de la ejecución del contrato, previo aval del supervisor a través de la plataforma SECOP II.
- El contratista deberá entregar los diagramas de flujo del diseño del sistema en un plazo máximo de un (1) mes calendario a partir del inicio de la ejecución del contrato.
- El contratista deberá presentar el cronograma del servicio de soporte preventivo incluido en la solución en un plazo máximo de un (1) mes calendario a partir del inicio de la ejecución del contrato.
- El contratista deberá entregar un documento que certifique las fechas de inicio y terminación del soporte, en un plazo máximo de ocho (8) días calendario a partir del inicio de la ejecución del contrato.

Nota:

- Todos los entregables y documentos generados en el marco del contrato serán de propiedad del Distrito de Medellín y deberán presentarse en idioma español.
- Los documentos producidos o generados por el fabricante podrán ser entregados en idioma inglés.

9. ACUERDOS DE NIVELES DE SERVICIO (ANS).

De acuerdo con su naturaleza, los incidentes de soporte se clasificarán en las siguientes categorías: críticos, importantes, normales y menores. En consecuencia, su atención deberá regirse conforme a las prioridades establecidas a continuación:

- **Prioridad 1 (Crítico):** Se presenta cuando la red se encuentra inoperativa o el impacto sobre la operación es crítico. En estos casos, todas las partes involucradas deberán asignar recursos de tiempo completo para la solución del incidente, conforme al nivel de servicio adquirido.

  En un plazo máximo de una (1) hora, contada a partir del reporte del incidente por cualquiera de los canales habilitados, un ingeniero experto y certificado en la tecnología deberá establecer contacto con el personal designado por la Subsecretaría de Servicios de Tecnologías de la Información del Distrito de Medellín, con el fin de iniciar la solución del problema.

  En caso de ser necesario, el incidente deberá escalarse, garantizando la atención en sitio por parte de un ingeniero experto y certificado en un plazo máximo de cuatro (4) horas adicionales.

- **Prioridad 2 (Importante):** Se presenta cuando la operación de los servicios se encuentra severamente degradada o cuando aspectos relevantes del negocio se ven afectados negativamente. En estos casos, las partes deberán asignar recursos durante el horario de oficina para atender la situación.

En un plazo máximo de cuatro (4) horas, contadas a partir del reporte del incidente, un ingeniero experto y certificado deberá establecer contacto con el personal designado por la Subsecretaría de Servicios de Tecnologías de la Información del Distrito de Medellín, con el fin de gestionar la solución del problema.

Si el caso lo amerita, deberá escalarse, garantizando la atención en sitio en un plazo máximo de veinticuatro (24) horas.

- **Prioridad 3 (Normal):** Se presenta cuando el desempeño operativo se encuentra afectado, pero las operaciones del negocio continúan funcionando. Las partes deberán asignar recursos dentro del horario de oficina para restablecer el servicio a niveles adecuados.

  En un plazo máximo de setenta y dos (72) horas, contadas a partir del reporte del incidente, un ingeniero experto y certificado deberá establecer contacto con el personal designado por la Subsecretaría de Servicios de Tecnologías de la Información del Distrito de Medellín, con el fin de avanzar en la solución del problema.

  Si se requiere, el incidente deberá escalarse, garantizando la atención en sitio en un plazo máximo de noventa y seis (96) horas.

- **Prioridad 4 (Menor):** Se presenta cuando se requiere información o asistencia relacionada con las capacidades, instalación o configuración de la solución. Las partes deberán asignar recursos dentro del horario de oficina para atender el requerimiento. La atención y solución del requerimiento deberán realizarse en un plazo máximo de noventa y seis (96) horas, contadas a partir de su registro.

  Nota:

  En caso de presentarse incumplimientos o retrasos en el cumplimiento de los Acuerdos de Niveles de Servicio (ANS) definidos anteriormente, que sean atribuibles al contratista y que, a juicio del supervisor del contrato, pongan en riesgo la continuidad en la prestación del servicio, dicha situación deberá ser consignada en el informe de supervisión correspondiente, con el fin de dar inicio al proceso administrativo sancionatorio a que haya lugar, de conformidad con la normatividad vigente aplicable.

10. TRANSFERENCIA DE CONOCIMIENTO

- El contratista deberá desarrollar cuatro (4) sesiones de transferencia de conocimiento y sensibilización, dirigidas a un mínimo de diez (10) funcionarios de la entidad, con el propósito de fortalecer la comprensión del funcionamiento y la administración de la plataforma de la solución de Filtrado de Contenido Web (SWG). Asimismo, estas sesiones deberán contribuir a la identificación de situaciones sospechosas que permitan mitigar la propagación de software malicioso en la plataforma tecnológica.

Las sesiones podrán realizarse de forma virtual, con una duración total de ocho (8) horas, y deberán ser programadas por el supervisor del contrato durante el primer trimestre, contado a partir del inicio de la ejecución del contrato, previa concertación con el proveedor.

- El contratista deberá realizar reuniones de consultoría con una periodicidad mensual de (4) horas remotas, cada una con una duración de dos (2) horas, en las cuales deberá informar sobre la incorporación de nuevas características en la solución, así como la forma de aprovecharlas. Igualmente, deberá brindar orientación sobre el tratamiento de amenazas, incluyendo las modificaciones definidas por el fabricante para su gestión, y presentar las mejores prácticas a implementar con el fin de mitigar riesgos en la plataforma tecnológica.

- Adicionalmente, el contratista deberá proponer acciones de mejora orientadas a las plataformas existentes en el Distrito y en el conglomerado público, con el fin de generar sinergias en los procesos y sistemas de la entidad. Lo anterior, en cumplimiento del Decreto 0310 de 2022, mediante el cual se reglamenta el Acuerdo 016 de 2020, denominado “Modelo de compras públicas socialmente responsable”.

11. OTRAS CONSIDERACIONES

Las siguientes consideraciones deberán estar incluidas en la propuesta:

El contratista deberá especificar, dentro de los documentos entregados (manuales, datasheets y demás documentación relacionada), el apartado en el cual se evidencie el cumplimiento de cada uno de los requerimientos establecidos, indicando de manera expresa si cada ítem de la propuesta es certificado.

12. CANTIDADES PROYECTADAS

La propuesta económica deberá presentarse discriminada por ítems, conforme a la siguiente estructura:

DESCRIPCIÓN	CANTIDAD
Renovación: Skyhigh SWG Anti-Malware AddOn (12 Meses)	7001
Renovación: Skyhigh SWG Software - Subscription (12 Meses)	7001
Renovación: Advanced RMA (next business day ship) Hardware Support (12 Meses)	1
Renovación: Skyhigh SWG (12 Meses)	1001
Renovación: Trellix ePO-SaaS for SSE - AddOn (12 Meses)	1001
Renovación: Skyhigh SWG (8 Meses)	2001
Renovación: Trellix ePO-SaaS for SSE - AddOn (8 Meses)	2001
Adquisición: Skyhigh SWG WG5500-F Appliance (12 Meses)	1
Adquisición: Advanced RMA (next business day ship) Hardware Support (12 Meses)	1
Soporte platinum 7X24 con visitas de mantenimiento mensual de (4) horas remotas.	12
Servicios de implementación 5x8 remotos más Gte de proyectos y transferencia de conocimiento de cuatro horas.	1