Objeto:
Adquirir soporte y actualización de un sistema de Filtrado de Contenido Web SWG

Alcance del objeto:
Por medio de este proceso de contratación se pretende contratar la adquisición soporte y actualización de un sistema de Filtrado de Contenido Web SWG por un año, de acuerdo a 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.

ESPECIFICACIONES TÉCNICAS.

La solución deberá cumplir con:

Actualmente se tiene una Plataforma de Filtrado de Contenido McAfee Web Gateway (SWG), la cual está compuesta por 2 Appliances de la referencia WG 5500D y WG 5500E:

- El Appliance referencia WG 5500D se le debe renovar la garantía por 12 meses, a partir de su vencimiento.
- El Appliance referencia WG 5500E se le debe renovar la garantía por 12 meses, a partir de su vencimiento.

1. SOFTWARE Y LICENCIAMIENTO.

- El licenciamiento solicitado debe ser por 12 meses y debe ser bajo la modalidad:
- Mínimo 8000 usuarios nombrados.
- Sistema operativo de los Appliance es Linux Endurecido o propio del fabricante.
- Licencias de equipo, software servidor y clientes deben proveerse a perpetuidad, sin costo de licenciamiento adicional. Es decir, la maquina no podrá dejar de funcionar sino se renueva el contrato de soporte, entendiendo que los módulos de actualización no quedaran operativos (nuevas categorías de filtrado, listas negras, nuevas versiones de Firmware, actualización de malware).
- El licenciamiento debe ser completo teniendo en cuenta servidores y host que van a ser parte de la solución; así mismo incluyendo su familia de productos que complementen la herramienta.
- No se aceptará software cliente instalado en las estaciones de trabajo, salvo para equipos que no se encuentren en la red corporativa.

2. SOPORTE.

- El servicio de soporte debe ser prestado por personal certificado en la solución.
- Soporte por 12 meses para atención a toda la Plataforma de Filtrado de Contenido Web.
- El contratista en la atención de los casos de soporte debe reportar su número de caso y el número de caso del fabricante.
- No se pueden cerrar los requerimientos (Casos de Soporte – Tickets) hasta que el supervisor del contrato autorice.
- Realización de visitas que sean necesarias para solucionar incidentes.
- El contratista debe garantizar que los hallazgos o mejoras detectados en la herramienta donde el fabricante debe escalar el requerimiento a su área de desarrollo porque generan dificultades

en el servicio, bajando la credibilidad del producto y calidad del servicio, deben ser solucionados de acuerdo a los ANS.

- El contratista debe garantizar que el tiempo que se demore el fabricante solucionando alguna falla en el software que tuvo que escalar a su área de desarrollo, sea compensado en tiempo sobre el vencimiento de las licencias y el soporte.
- Las actividades de actualización que se requieran se deberán programar en horarios previamente autorizados por el Distrito de Medellín (horarios no laborales) y estos serán desarrollados por el contratista, quien deberá entregar el plan de trabajo respectivo.
- Servicio on-line de desbloqueo sin costo adicional.
- El servicio de soporte para los incidentes reportados debe ser atendido según los ANS.
- El contratista debe garantizar que la atención vía telefónica, correo electrónico, Soporte Remoto y/o chat por parte del fabricante sea con disponibilidad 5x8, de lunes a viernes de 8am a 12pm y de 1pm a 5pm, durante la vigencia del contrato.
- Debe haber un acompañamiento en actualizaciones y/o mejoras previamente acordadas con el contratista en horario diferente al de la atención 5x8, sin costo adicional para el Distrito de Medellín, ya que estas actualizaciones no se pueden realizar en horario laboral.
- Las actualizaciones de firmware realizadas por el fabricante durante el periodo del contrato deberán estar incluidas en el presupuesto y el proveedor debe apoyar el montaje de dichos firmware.

3. ESPECIFICACIONES PLATAFORMA.

3.1. La solución debe conservar las siguientes características:

- El producto no puede estar en End of Sale en los próximos 3 años.
- La plataforma debe ser compatible con direccionamiento IP versión 6
- Compatibilidad para los Windows (7/ 8 / 8.1 / 10 / 11) Windows Server (2003 / 2008 / 2008 R2 / 2012) en versiones de 32 y 64 Bits, Linux en versiones de 32 y 64 Bits.
- Integración con LDAP basada en roles, la solución se debe integrar con toda la clase de servidores de LDAP tales como OpenLDAP, Lotus Domino, iPlanet LDAP y Windows Active Directory.
- La solución deberá poder integrarse con un Active Directory de Microsoft sin necesidad de instalar algún componente en los controladores de dominio. Esta integración permitirá que la administración de la solución se efectué por medio de cuentas de usuarios y grupos de administración basadas en el Active Directory.
- Administración Basada en Roles: Es requisito indispensable que se pueda segregar la administración de la seguridad diferenciando claramente los roles de Seguridad de Sistemas y de otras unidades definidas en el Active Directory. La solución deberá permitir la segregación de funciones de forma granular, permitiendo así definir al alcance o posibilidades de gestión para cada administrador.
- Los componentes de software y sus actualizaciones deben soportarse con el hardware y software existente en el Distrito de Medellín, en caso contrario el proveedor debe suministrar y correr con todos los gastos del hardware necesario para que el producto funcione adecuadamente.
- Personalización de la configuración si es necesario.
- Administración por GUI y CLI.
- La solución deberá permitir monitoreo en tiempo real de navegación.

- Conexión e integración con SAN y NAS o Servidor de archivos, para el almacenamiento o compartición de históricos de reportes.
- Autenticación por Kerberos y NTLM
- Soporte envío syslog a un SIEM o uno que realice las tramas similares a un syslog.
- La solución deberá poder realizar respaldos y restauraciones de las configuraciones.
- La solución tendrá la capacidad de presentar al usuario, una página web con mensajes modificables por los administradores del sistema, en caso de algún problema o infracción.
- Las políticas, los cuadros de mando, informes y más deberán estar disponibles en una consola o menú gráfico, para reducir el tiempo y la experiencia necesaria para lograr resultados.
- Compatibilidad con los diferentes navegadores de internet (Internet explorer 10 y superior, Chrome, Mozilla Firefox, opera, edge, safari).

3.2. Políticas de filtrado de contenido:

- La solución deberá tener la capacidad de utilizar expresiones regulares para la creación de las políticas
- La solución deberá tener la capacidad de utilizar expresiones booleanas para la creación de políticas.
- La solución deberá tener la capacidad de utilizar las políticas en forma anidadas o encadenadas.
- Web Proxy explícita y transparente con múltiples autenticaciones.
- La herramienta debe permitir la ruptura de certificados SSL para páginas que usan el protocolo HTTPS.
- Debe poseer lista negra y lista blanca de sitios web que se actualice automáticamente, pero también con la posibilidad de poder agregar manualmente.
- Motor de análisis de contenido que permite determinar por asociación de palabras claves si el contenido debe figurar o no en la página de Internet.
- Detección y gestión de las palabras clave prohibidas: reemplazo por caracteres de sustitución, o bloqueo de la página, o identificación en la URL y bloqueo de la misma.
- Debe permitir la priorización de las políticas de filtrado en función a su criticidad para la empresa.
- Monitoreo completo de puertos, control para aplicaciones y protocolos.
- Debe contener capacidad de mínimo 70 categorías predeterminadas o más de filtrado.
- Debe permitir configurar categorías propias.
- Permitir y denegar de adjuntar archivos en la web.
- Permitir y denegar descargar archivos en la web.
- La solución deberá permitir el bloqueo de Streaming Media.
- La solución debe filtrar de manera granular incluyendo las redes sociales como Facebook, Instagram, Twitter, Pinterest, Google+ y demás, de manera que se puedan bloquear acciones como: chatear, postear, ejecutar aplicaciones, compartir, subir fotos o archivos, compartir contenidos.
- Poder controlar el tráfico Peer to Peer y los protocolos que ellos usan.
- La solución deberá permitir el filtrado de tráfico no HTTP, como puede ser el de los programas P2P (eMule, etc.) o IM (mensajería instantánea).
- Poder controlar el acceso a aplicaciones y mensajería como Skype.

- Aplicación de funciones de filtrado al contenido a los protocolos y a las aplicaciones tipo: chat, newsgroups, programas de telefonía en línea, plataformas de descarga peer to peer, mensajerías instantáneas, etc.
- La solución permite inspeccionar el tráfico tanto de entrada como de salida de los protocolos HTTP, HTTPS, FTPS, y FTP.
- La plataforma debe alojar en cache las páginas web.
- Al ingresar a un FTP se debe permitir observar todas las funcionalidades de la página como: las actualizaciones de fechas y modificaciones de los directorios para los sitios que lo tengan habilitado.
- La aplicación de las políticas debe ser en tiempo real, no debe depender de que el usuario cierre y vuelva y abra su navegador.
- Ruptura de certificados SSL para filtrado de estos sitios

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

- Las políticas de accesos deberán estar basadas en: Dirección IP, Rango de Direcciones IP, Subredes y CIDR, Usuarios del Active Directory, Grupos de Usuarios del Active Directory, unidades organizativas (OU), grupo de Directorio Activo y segmentos de red.
- Las políticas de filtrado deben permitir, ver un video o grupos de videos (canales), aún si la categoría se encuentre bloqueada.
- Las políticas de filtrado deben permitirse para: IP, Nombre maquina (registro en el DNS), usuario Directorio Activo.
- Se debe poder definir un número ilimitado de perfiles, que permitan combinarlos con parámetros para el filtrado web como: horarios, tipos de archivo, listas personales, desbloqueo, duración de tiempo, capacidad de consumo en MB.
- La solución debe permitir filtrar por usuario o por grupo de usuarios de acuerdo a la capacidad de consumo de un sitio web específico o de alguna categoría.
- La solución debe permitir filtrar por usuario o por grupo de usuarios de acuerdo al tiempo de consumo de un sitio web específico o de alguna categoría.
- La solución debe permitir el control de cuotas para los usuarios por tiempo consumido.
- La solución debe permitir el control de cuotas para los usuarios en cantidad de bytes por un tiempo específico.
- La solución deberá soportar la configuración de tiempos de conexión mediante la configuración de reglas específicas.
- Control de límites de tiempo con múltiples opciones de autenticación para usuarios y grupos.
- La solución deberá tener la capacidad de filtrado por: por reputación de archivos, Tamaño del archivo, Extensión del archivo, Encabezados, Usuario o Grupo que realiza la descarga
- La solución debe permitir filtrar el acceso por subdominios de una URL
- La solución debe permitir filtrar el acceso por directorios de una URL

3.4. Protección antimalware:

- Protección de phishing y suplantación de sitios web.
- Debe permitir proteger a los usuarios de virus, spyware, troyanos, scams, malware, phishing, botnets, gusanos que infecten los equipos de cómputo.

- Evaluación en tiempo real de los contenidos, guiones y otros potenciales componentes de amenaza.
- La solución deberá contar con mínimo dos motores Antimalware.
- La solución deberá permitir la detección de malware entrante y saliente de la red.
- Las firmas deberán ser actualizadas automáticamente o bajo demanda de los administradores.
- La solución deberá permitir la detección heurística proactiva.

3.5. Actualizaciones:

- Actualización automática en tiempo real de las listas y parámetros por paquetes incrementales continua.
- Recibir actualizaciones inmediatas de nuevas amenazas por el periodo contratado.
- Migración a nuevas versiones estables de la herramienta.
- Las actualizaciones de firmware y las migraciones a otras versiones de la herramienta que sean necesarias deben ser informadas y los servicios prestados de instalación deben ser soportados por el contratista y su fabricante bajo su responsabilidad durante el periodo del contrato y deberán estar incluidas en el presupuesto.
- Las actualizaciones de los filtros por reputación de URL deben actualizarse en tiempo real continuamente, inmediatamente después que hayan sido descubiertas por el fabricante.
- La plataforma deberá mantenerse en la última versión estable.

Notas:

Todos los trabajos de actualización de firmware deben ser notificados y documentados oportunamente y otorgar su debido acompañamiento.

Las nuevas funcionalidades integradas en las actualizaciones deben ser notificadas y documentadas al supervisor del contrato

3.6. Reportes:

- El módulo de reportes debe estar incluido en la solución, sin costo adicional.
- La plataforma deberá identificar si una política está siendo usada, reportando la cantidad de coincidencias que se realizan en un periodo de tiempo determinado por usuario o por grupos.
- Reportes predefinidos.
- Generación de informes dinámicos los cuales pueden ser diarios, semanales y mensuales teniendo disponibilidad de datos en archivos planos y envió automático del reporte.
- Poder consultar a que política pertenece algún grupo, dirección IP o usuario.
- La herramienta debe de permitir exportar las políticas que se tengan implementadas mediante reportes (en excel, pdf, cvs, txt) teniendo en cuenta la prioridad de aplicación de las mismas.
- La herramienta debe permitir exportar todo tipo de informes así sean mayores a 5.000 registros y convertirlos a formatos como PDF, TXT, CSV, etc.
- La herramienta debe permitir importar listas de acceso, políticas y mapeos.
- Presentación de informes que permiten detectar el malware.
- Reporte del uso de ancho de banda utilizado por usuario o por grupos.
- La solución deberá permitir generar reportes históricos.

- La solución deberá permitir generar reportes de actividad de los usuarios.
- La solución deberá permitir generar reportes de los sitios bloqueados.
- La solución deberá tener la capacidad de enviar reportes programados por correo electrónico.
- Información para análisis forenses sobre quién, qué, dónde, cómo; captura de datos para incidentes de seguridad.
- Poder visualizar el comportamiento del procesador, memoria, capacidad del equipo en tiempo real

4. INSTALACIONES O CONFIGURACIONES.

- La instalación o configuración de la solución que abarque los equipos servidores Appliance (Hardware), en caso de llegar a requerirse (por ejemplo en caso de cambio por garantía), debe ser en sitio por personal certificado en la solución.
- La instalación o configuración para los agentes de licenciamiento (Software), esta deberá estar a cargo de personal certificado en la solución.
- Integración de la herramienta con la infraestructura disponible.
- Realización y verificación de pruebas de integración.
- La instalación del programa se debe efectuar en el ordenador principal de la red sobre el cual está instalado un compartimiento de conexión. La conexión de otros ordenadores (en modo "esclavo") será filtrada a través del ordenador maestro sin tener que instalar el programa en todos los demás ordenadores.
- Ruptura de certificados SSL para filtrado de estos sitios, mínimo 5.

Nota: Todas las actividades anteriores se deben realizar en las instalaciones del Distrito de Medellín sin costo para este.

Si la solución o herramienta posee problemas debe haber atención en sitio tiempo completo hasta que entreguen una solución real confiable y estable.

5. GARANTÍA DE LA SOLUCIÓN.

- Garantía que requiere el Distrito de Medellín a nivel de hardware es: los 2 Appliances de referencia WG 5500D y referencia WG 5500E deben contar con garantía por 12 meses, a partir de su vencimiento.
- Garantía de 12 meses para el software a partir del momento de recibo a satisfacción, entrega en operación u ultimo vencimiento.
- En caso de reemplazo, el envío debe realizarse de inmediato a la notificación del Distrito de Medellín, y todos los gastos de envío, nacionalización y demás serán a cargo del contratista.
- Posibilidad de migración a nuevas versiones.
- Permitir montar servidores virtuales como plan de contingencia, sin tener que pagar un licenciamiento adicional, en caso de presentarse una falla que afecte el servicio indefinidamente.
- Si por algún motivo se detecta que la herramienta tiene fallas en su hardware, el contratista debe asumir totalmente los costos de cambio o actualización de ello como memoria, procesador, disco duro u otros componentes.
- Posibilidad de migración a nuevas versiones.

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

- **Soporte correo electrónico**: Respuesta a través de un buzón de correo electrónico de soporte informado con anticipación, y deberá ser atendido de acuerdo a la criticidad del problema, si el buzón es modificado deberá ser informado este con anterioridad el cambio.

- **Soporte telefónico**: Si el número telefónico o los números telefónicos informados cambian estos debe ser especificados con anterioridad, y deberá ser atendido de acuerdo a la criticidad del problema.

- **Soporte Remoto**: Para conectarse remotamente con el hardware, deberá contar con previa autorización, con el fin de garantizar la seguridad y control en el acceso.

- **Soporte por chat:** Deberá ser atendido de acuerdo a la criticidad del problema, si el chat es modificado deberá ser informado este con anterioridad el cambio.

7. ENTREGABLES.

- Certificación de garantía por 12 meses para el hardware y el software, a partir de su vencimiento, plazo 8 días calendario a partir de la fecha de inicio de ejecución por parte del supervisor a través de la plataforma SECOP II.
- Manuales y documentación actualizada de la última versión para la administración, configuración, parametrización e instalación de la solución implementada en el Distrito de Medellín, plazo 8 días calendario a partir de la fecha de inicio de ejecución por parte del supervisor a través de la plataforma SECOP II.
- Plan de contingencia para la plataforma, plazo 1 mes calendario a partir de la fecha de inicio de ejecución por parte del supervisor a través de la plataforma SECOP II.
- El contratista deberá suministrar datos de contacto para soporte y un instructivo de cómo generar los casos, plazo 8 días calendario a partir de la fecha de inicio de ejecución por parte del supervisor a través de la plataforma SECOP II. Para este punto cabe aclarar que si algún canal para colocar un soporte cambia este documento debe ser actualizado inmediatamente.
- Plan de trabajo y metodología de implementación de la solución, el cual contenga el reporte de las acciones a tomar, se debe entregar inmediatamente se realice inicio de ejecución por parte del supervisor a través de la plataforma SECOP II.
- Diagramas de flujo del diseño del sistema, plazo 1 mes calendario a partir de la fecha de inicio de ejecución por parte del supervisor a través de la plataforma SECOP II.
- Cronograma de servicio de soporte preventivo incluida en la solución, plazo 1 mes calendario a partir de la fecha de inicio de ejecución por parte del supervisor a través de la plataforma SECOP II.
- Documento que certifique fecha de inicio y terminación del soporte, plazo 8 días calendario a partir de la fecha de inicio de ejecución por parte del supervisor a través de la plataforma SECOP II.

Nota: Todos los entregables y documentos generados en el marco del contrato serán de propiedad del Distrito de Medellín y deben ser en español y todos aquellos documentos producidos o generados por el fabricante, podrán ser entregados en el idioma inglés.

8. ACUERDOS DE NIVELES DE SERVICIO (ANS).

De acuerdo con su naturaleza, los incidentes de soporte se pueden clasificar como: Críticos, importantes, Normales o menores; por lo tanto, la atención será regida bajo las siguientes prioridades:

- **Prioridad 1 (Critico):** La red está "caída" o el impacto sobre su operación es crítico. Todas las partes involucradas se comprometen a dedicar recursos de tiempo completo, de acuerdo al nivel adquirido, para resolver la situación. Máximo una (1) hora después de reportado el incidente por alguno de los medios de comunicación, un ingeniero experto y certificado en tecnología debe comunicarse con el personal encargado de los equipos en cuestión de la Subsecretaria de Servicios de Tecnologías de la Información del Distrito de Medellín, para otorgar la solución del problema, si el caso lo amerita debe ser escalado para que en el transcurso de las siguientes cuatro (4) horas a un ingeniero experto y certificado en esta tecnología otorgue solución del problema en sitio.

- **Prioridad 2 (Importante):** La operación de los canales está severamente degradada o aspectos importantes de la operación del negocio se ven afectados negativamente por el desempeño inadecuado de estos. Todas las partes involucradas se comprometen a dedicar recursos de tiempo completo durante las horas de oficina estándares para resolver esta situación. Máximo cuatro (4) hora después de reportado el incidente por alguno de los medios de comunicación, un ingeniero experto y certificado en tecnología debe comunicarse con el personal encargado de los equipos en cuestión de la Subsecretaria de Servicios de Tecnologías de la Información del Distrito de Medellín, para otorgar la solución del problema, si el caso lo amerita debe ser escalado para que en el transcurso de las siguientes veinticuatro (24) horas a un ingeniero experto y certificado en esta tecnología otorgue solución del problema en sitio.

- **Prioridad 3 (Normal):** El desempeño operativo de los canales está deteriorado, mientras que las operaciones del negocio funcionan normalmente. Las partes comprometen recursos durante las horas de oficina normales para restaurar el servicio a niveles satisfactorios. Máximo setenta y dos (72) horas después de reportado el incidente por alguno de los medios de comunicación, un ingeniero experto y certificado en la tecnología debe comunicarse con el personal encargado de los equipos en cuestión de la Subsecretaria de Servicios de Tecnologías de la Información del Distrito de Medellín, para otorgar la solución del problema, si el caso lo amerita debe ser escalado para que en el transcurso de las siguientes noventa y seis (96) horas a un ingeniero experto y certificado en esta tecnología otorgue solución del problema en sitio.

- **Prioridad 4 (Menor):** Se requiere información o asistencia sobre las capacidades de los productos, o sobre Instalación o configuración. Las partes se comprometen a entregar recursos durante las horas de oficina normales para entregar la información o el soporte requerido. Máximo en noventa y seis (96) horas debe ser atendido y solucionado el requerimiento.

En caso de presentarse retrasos en el cumplimiento de los acuerdos de niveles de servicio detallados anteriormente, que sean atribuibles al contratista y que a juicio del supervisor del contrato pongan en riesgo la continuidad en la prestación del servicio, se procederá a plasmar en informe de supervisión la situación presentada, con el fin de iniciar el correspondiente proceso

administrativo sancionatorio a que haya lugar, de conformidad con la normatividad que rige la materia

9. OTRAS CONSIDERACIONES

Las siguientes consideraciones deben estar incluidas en la propuesta:

- Se debe especificar en los documentos entregados en que parte de sus manuales, datasheet's y documentos relacionados, cumple con cada requerimiento y si certifica cada ítem de la propuesta.

10.CANTIDADES PROYECTADAS

La propuesta económica debe venir discriminada en Ítems de la siguiente manera:

#	DESCRIPCIÓN
1	Valor de la renovación del licenciamiento
2	Valor del Hardware Support del nuevo Appliance (Garantía)
3	Valor del soporte de la solución por los 12 meses