ANEXO TÉCNICO

1. DENOMINACIÓN DEL BIEN O SERVICIO

OBJETO CONTRACTUAL: Adquisición, instalación y puesta en marcha de una plataforma de protección para estaciones de trabajo, servidores y equipos de trabajo móviles (NGAV) que permita a la organización reforzar su postura de seguridad mediante la protección de sus activos en las diferentes ubicaciones donde la organización tiene presencia.

2. CÓDIGO ESTÁNDAR DE PRODUCTOS Y SERVICIOS DE NACIONES UNIDAS (UNSPSC, V.14.080)

SEGMENTO	FAMILIA	CLASE	PRODUCTO
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43230000 Software	43231500 Software funcional específico de la empresa	43231512 Software de manejo de licencias
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

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

<table>
<tr><th>Ítem</th><th>Descripción</th></tr>
<tr><td>Licenciamiento requerido por un año:</td><td>El proveedor deberá proporcionar la adquisición de 1300 licencias Antivirus
<table><tr><th>N°</th><th>DESCRIPCIÓN</th><th>Cantidad</th></tr><tr><td>1</td><td>Adquisición de licencias de un antivirus para estaciones de trabajo por un (1) año.</td><td>1300</td></tr></table></td></tr>
<tr><td>Referencia plataforma</td><td>Nombre del producto: _____
Versión del producto: _____</td></tr>
<tr><td>Características Técnicas</td><td>La herramienta Antivirus debe contemplar los siguientes requerimientos como mínimo:
<table><tr><th>Descripción</th></tr><tr><td>Proveer 1300 licencias para protección de Antivirus para estaciones de trabajo por un (1) año, las cuales podrán ser usadas en los diferentes sistemas operativos como: Windows 7, Windows 8, Windows 10 Pro, Windows 11, 64bits,</td></tr></table></td></tr>
</table>

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

CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

		Las políticas de antivirus definidas desde la consola deben poder ser aplicables para cualquier sistema operativo soportado, para usuarios del directorio activo, usuarios locales o usuario fuera del dominio.
		La solución debe contar con un mecanismo de actualización que garantice la integridad y minimice la manipulación o alteración de las definiciones de virus por medio de cifrado y firmas digitales.
		La solución debe contar con tecnología de remoción y detección de virus, macros, troyanos, gusanos, ransomware y en general todo tipo de códigos maliciosos.
		La solución deberá ser estable, de tal manera que no afecte ni perjudique el rendimiento de las máquinas y/o aplicativos que estén instalados en las mismas.
		La solución debe contar y quedar configurada con un módulo de exploración en tiempo real, que ofrezca protección continúa frente a los virus que llegan a través de dispositivos de almacenamiento extraíbles, en la red y de las diversas fuentes en Internet.
		La solución debe tener la capacidad de explorar los procesos que se encuentren corriendo en memoria.
		La solución debe explorar múltiples formatos de compresión de archivos como: (zip, rar, tar, gzip entre otros).
		La solución debe permitir la creación de tareas centralizadas de revisión y limpieza de archivos del sistema.
		La solución debe tener la capacidad de poder configurar una segunda opción de actualización de firmas, en caso de que la primera opción llegue a fallar.
		El motor de exploración deberá utilizar distintas tecnologías de detección virus: Exploración de firmas y exploración heurística "busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos".
		La solución debe poder detectar comunicaciones a sitios de comando y control con el fin de evidenciar pérdidas de información en los clientes.
		La solución debe contar con los mecanismos de protección para no poder ser desinstalada o desactivada por el usuario.
		La solución debe avisar sobre los posibles conflictos que existan de la solución a otras soluciones de anti-virus y firewall instalados previamente en la máquina.
		Se deben poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.
		Se debe poder restringir completa o parcialmente el acceso a la consola cliente para configurar parámetros individuales sobre el host.
		La solución debe basarse en una plataforma común sobre la cual se incorporan módulos de Prevención de amenazas, y Firewall de escritorio, y que permita el intercambio de información entre cada uno de los módulos.
		La solución debe poder configurarse para realizar escaneos por demanda o programados, desde la consola de administración o desde la consola cliente
		Se deben reportar eventos de amenazas directamente sobre la consola cliente y visibles desde la consola de administración de la solución.
		La solución debe poder habilitar la opción de escaneo de click-derecho sobre carpetas específicas en sistemas operativos soportados.
		La solución debe contar con mecanismos de protección a ejecución de scripts maliciosos de Internet Explorer, sean JavaScript o VBScript.

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

SYSTEM CERTIFICATION ISO 9001 SGS CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

		El sistema debe permitir la detección basada en el comportamiento anómalo en el punto final.	
		Contener aplicaciones desconocidas impidiéndoles realizar cambios a nivel del sistema, mediante reglas de Protección de acceso a aplicaciones y monitoreo de procesos en ejecución desconocidos.	
		La solución debe emplear una arquitectura multicapa, para defenderse de ataques basados en comportamientos, evitando cambios a nivel de sistema, restringiendo el acceso a procesos, archivos, recursos compartidos, valores y claves de registro.	
		La solución debe ser compatible con todas las versiones de los navegadores Internet Explorer, Google Chrome, Mozilla Firefox, safari, Internet Explorer Edge, entre otros.	
		Disponer de un motor antimalware que detecte infecciones y analice virus, gusanos, spyware, malware, ransomware y otras amenazas ubicadas en las estaciones de trabajo.	
		Proteger las estaciones de trabajo contra infecciones a través descargas de internet, archivos adjuntos de e-mail, redes, archivos compartidos, CD-ROM, USB, dispositivos extraíbles, carpetas públicas y carpetas personales de todo tipo de correo, almacenadas localmente, mensajes de correo electrónico entrante y saliente, servicios en línea, entre otros tipos de almacenamiento.	
		La solución debe ser instalada configurada y gestionada en cada estación de forma centralizada desde los servidores, sin tener que hacer un despliegue uno a uno.	
		La solución debe permitirle al administrador las opciones de preguntas en cuanto a limpiar, borrar, denegar acceso, e inclusive debe manejar una carpeta de cuarentena para archivos infectados que se detecten a través de reglas y lista predefinidas y/o personalizadas por el administrador.	
		La solución debe tener la capacidad de generar exclusiones por nombre de archivos, carpetas y tipos de archivos.	
		Debe contar con medidas de seguridad para que el usuario o cliente no pueda modificar políticas corporativas efectuadas desde la consola de administración.	
		La solución debe ser capaz de detectar el 100% de los virus conocidos (reportados en listas), contra programas malignos especificados.	
		Debe realizar los informes detallados con los datos referentes a la detección de virus tanto en tiempo real, como del análisis bajo demanda y programado.	
		Análisis en tiempo real en los dispositivos extraíbles antes de tener acceso a ellos una vez conectados a los equipos de cómputo.	
		La solución debe contar con mecanismos de protección de amenazas avanzadas tipo ransomware.	
		La solución debe contar con mecanismos de borrado seguro de malware residente en memoria que sean difíciles de erradicar, evitando el reinicio de servidores críticos.	
		Debe contar con tecnología de mitigación de EXPLOITS, que ataquen soluciones comúnmente usadas y que pueden no estar actualizadas, corno acrobat, flash player, entre otras	
		La solución debe contar con la aplicación de políticas de acuerdo con la identificación de la red a la cual se encuentre conectada la máquina.	
		La solución de Control de Dispositivos debe permitir auditar la conectividad de los dispositivos de almacenamiento externo.	
		La solución de Control de Dispositivos debe poder ser desplegada de manera	

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

SYSTEM CERTIFICATION ISO 9001 SGS CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

		centralizada, a través de la consola de administración o a través de herramientas de distribución de terceros.
		La solución de Control de Dispositivos debe permitir la creación de excepciones para un usuario, maquina o dispositivo especifico.
		La solución de Control de Dispositivos debe permitir asignar reglas y políticas para usuarios y grupos de Directorio Activo, usuarios locales o usuario fuera del dominio.
		La solución de Control de Dispositivos debe tener la capacidad de monitorear la actividad de usuario de manera silenciosa.
		La solución de Control de Dispositivos debe permitir la creación y manejo de listas blancas y negras de dispositivos de almacenamiento extraíble, con base en la marca y el ID del dispositivo.
		Disponer de un motor antimalware o antispyware que detecte infecciones y analice virus, gusanos, y otras amenazas ubicadas en los servidores.
		Actualización diaria, incremental y automáticamente, así como patrones de comportamiento de los nuevos virus.
		Gestión centralizada y remota de la red con múltiples vistas gráficas de los servidores para un fácil reparto de las tareas entre los administradores, así como también se debe permitir funciones de acceso seguro (ZTNA) para el análisis de postura de seguridad (es decir, validación del sistema operativo actual, firewall del host, detección de procesos, software de antivirus) además de la identificación del activo, autenticación e identificación del usuario y validación que incluya funciones de CASB en línea unificados dentro del mismo agente.
		Análisis de ficheros comprimidos.
		Exclusión del análisis de extensiones o ficheros no deseados.
		Compatibilidad para descargar las actualizaciones desde Internet a través de las versiones seguras de los protocolos FTP y/o HTTP, colocándolas en múltiples repositorios distribuidos donde los clientes puedan buscar las definiciones de manera local, lo cual permite un ahorro en el ancho de banda.
		Capacidad de programar las actualizaciones para que sean realizadas en diferentes momentos y horas específicas (diaria, semanal, mensual, cuando la máquina este inactiva, inmediatamente, entre otras).
		Capacidad de actualizar automáticamente los archivos de definiciones de virus, motor antivirus, ficheros de firmas y actualizaciones del producto antivirus de forma: automática, centralizada e incremental.
		Capacidad de generar reportes ilimitados, detallados y personalizados por fecha, tipo de amenaza, amenazas detectadas y/o eliminadas, equipos infectados y/o desinfectados.
		La solución debe ser capaz de realizar Aislamiento del Endpoint en caso de malware o comportamientos sospechosos que puedan desencadenar un brote de malware.
		La consola de administración ofrecida por el proponente debe poder ser administrada en plataforma cloud u on-premise
		La solución debe integrarse vía API y/o nativamente con la plataforma de seguridad actual para tener un dashboard del estado de los dispositivos en tiempo real y manejar rápidamente cuarentenas de dispositivos infectados.
		La solución debe hacer un escaneo de las vulnerabilidades presentes en el equipo y hacer virtual patching de los hallazgos, reportándolos a la consola de gestión mientras se autoriza una corrección por parte del administrador.
		La solución debe ser capaz de bloquear aplicaciones, mediante un perfil editable, ya sea

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

SYSTEM CERTIFICATION ISO 9001 SGS CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

	instaladas o en modo portable, para evitar la ejecución de programas, desarrollos o protocolos orientados a evadir la acción del control del Antivirus. La solución deberá enviar a la consola de gestión un inventario del software instalado en cada dispositivo con el fin de identificar programas y versiones de estos que puedan comprometer la seguridad del dispositivo. La solución debe estar en capacidad de bloquear acceso a canales de YouTube, o bloquear páginas basada en la presencia de ciertas palabras o patrones. La solución debe estar en capacidad de enviar archivos maliciosos a una inspección tipo sandbox en la nube del fabricante o en premisas, para proteger contra nuevas amenazas, y poder actualizar la inteligencia de amenazas de acuerdo con el resultado de la inspección en el ambiente sandbox. La solución debe estar en capacidad de hacer filtrado web y 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. El oferente de la solución deberá aportar los catálogos de la solución donde se indica el número de página del cumplimiento de cada uno de los requerimientos técnicos de la solución. Se debe entregar junto con la propuesta la certificación emitida directamente de los fabricantes de las soluciones ofertadas donde se evidencie que son distribuidores autorizados y se encuentran en la categoría más alta del programa de canales del fabricante, estas cartas deben ser dirigidas a la Entidad. Las anteriores herramientas deben ser administrables a través de una consola web o on-premise con asignación de roles por privilegios, con su correspondiente licencia en caso de que aplique. El proveedor deberá realizar la implementación y parametrización de las soluciones a nivel de consola de administración para que estos sean gestionados por la Secretaría General de la Alcaldía mayor de Bogotá, realizando el despliegue de las soluciones en una muestra de equipos (de 30 equipos) para validar la configuración y funcionamiento de las herramientas y las reglas establecidas. De acuerdo con lo anterior, se ha de aclarar que el oferente de la solución deberá realizar la instalación, despliegue y puesta en marcha de la solución completa para los 1300 equipos de la entidad, antecediendo a los pilotos realizados en los 30 equipos de prueba comentados en el párrafo anterior. **NOTA:** Las soluciones se deben poder implementar en servidores físicos y/o virtuales, aclarando que la Secretaría General de la Alcaldía mayor de Bogotá, cuenta con una infraestructura para implementar las soluciones, la cual depende de los requerimientos de las herramientas cotizadas, se descartarán las soluciones que incluyan la adquisición de appliance o hardware para su funcionamiento.
Documentación	• Entregar dentro de los 5 días hábiles posteriores a la firma del acta de requerimiento de entrega del contrato, la documentación que evidencie adquisición del licenciamiento de cada una de las herramientas. • Entregar dentro de los 5 días hábiles posteriores a la firma del acta de requerimiento de entrega del contrato, el protocolo de soporte donde relacione en

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

CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

	detalle los canales de atención, el personal a cargo del contrato, los tiempos de respuesta, entre otros. • Entregar manuales técnicos, funcionales o cualquier documento asociado al uso y configuración de la herramienta una vez sea activada la licencia y cuando exista una actualización sobre esta. • Atender los requerimientos de soporte en el lugar de ubicación de la licencia o por vía remoto según solicitud la Secretaría General de la Alcaldía mayor de Bogotá, durante el tiempo de soporte. • Suscribir acuerdo de confidencialidad
Afinamiento	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. El afinamiento debe contemplar actividades diferentes a la instalación y parametrización de la herramienta y debe contemplar actividades como las descritas a continuación: • Crear, validar y ajustar las reglas, políticas o reportes para determinar si son efectivas y cumplen con las necesidades de la SGAMB • Parametrización de Reportes y Módulos, siempre y cuando se encuentren dentro de la licencia de antivirus. • Pruebas de funcionamiento de las reglas. • Revisar que los backups configurados se están generando de forma correcta. • Verificar que no exista pérdida de información. • Revisar el uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la solución; revisar el uso y configuración de las herramientas de reportes y almacenamiento de logs. • Configuraciones para eventos masivos. • Responder las inquietudes de la Unidad relacionadas con afinamientos y cambios en la configuración de la solución. Los afinamientos se deben realizar de manera presencial en las instalaciones de la Unidad con acompañamiento de un colaborador asignado por la Secretaría General de la Alcaldía mayor de Bogotá, para esta actividad. En caso de que se requiera acceder de forma remota a los equipos de la solución, esto debe ser autorizado con el supervisor del contrato por parte de la Secretaría General de la Alcaldía mayor de Bogotá, con previa presentación y aprobación del plan a realizar. A los diez (10) días hábiles de efectuada alguna actividad el afinamiento, el contratista deberá entregar el informe técnico al personal designado por la Secretaría General de la Alcaldía mayor de Bogotá, con el resultado de las actividades realizadas, hallazgos y recomendaciones sobre la solución, con la relación de las horas ejecutadas.
Transferencias de Conocimiento	El contratista debe brindar transferencia de conocimiento acerca del manejo técnico y funcional, respecto al uso, administración y aprovechamiento del licenciamiento a renovar, con el objetivo de que la entidad adquiera conocimientos para la operación y programación de la solución tecnológica. Dicha trasferencia debe ser de mínimo (40) horas, para mínimo dos (2) personas por sesión y la cantidad de sesiones será acordada con la Supervisión del Contrato, en los horarios establecidos por la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., de lunes a viernes entre 7:00 a.m. a 4:30 p.m. Dichas sesiones deberán ser soportadas con el material utilizado (manuales, presentaciones y/o demo) y listados de asistencia. La transferencia de conocimientos debe ser brindada por personal certificado (La

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

SYSTEM CERTIFICATION ISO 9001 SGS CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

	certificación del profesional debe estar vigente al momento de realizar la sesión o sesiones de la transferencia de conocimientos) y se entregara certificado correspondiente a la Entidad.

3.1. ALCANCE Y DESCRIPCIÓN DEL SOPORTE

- La adquisición del licenciamiento (software y firmware) y de soporte con fabricante adquirido deben estar vigentes por un (01) año, contado a partir de la firma del acta de recibo a satisfacción, debe incluye acceso a garantía, actualizaciones por nuevas versiones liberadas y soporte técnico de fabricante.
- Deben entregar los documentos donde se acredite la titularidad y vigencia del licenciamiento del software o solución adquirida por la entidad (software y firmware) y de soporte con fabricante.
- El contratista deberá cumplir las actividades y los requisitos que se relacionan seguidamente:

    - Realizar la configuración y alistamiento de la solución a la última versión estable aprobada por el fabricante.
    - El contratista deberá realizar y documentar, las actividades previa coordinación con el supervisor del contrato entre otras: Configurar, afinar y revisar los reportes / logs de las plataformas y mantener actualizados los niveles de Firmware de acuerdo con las últimas versiones estables liberadas por el fabricante durante la ejecución del contrato.

- Soporte técnico y garantía de fabricante por un (01) año, contado a partir del acta de requerimiento de entrega. Esquema de atención 7X24X365 directamente con fabricante. El servicio de soporte debe incluir atención de incidentes, acompañamiento a nuevas implementaciones, actualizaciones, configuraciones de acuerdo con las necesidades de la secretaría general y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil.
- Actualizaciones: El contratista debe informar a la supervisión del contrato, respecto de las actualizaciones, una vez estas sean liberadas, y deberá aplicarlas en un tiempo no mayor a ocho (8) días calendario en coordinación y visto bueno de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC. En caso de que el contratista favorecido no informe de las nuevas actualizaciones liberadas, en ningún momento lo exonera de su instalación y deberá realizarlas así el contrato se encuentre liquidado o de lo contrario se aplicaran las pólizas establecidas. El contratista deberá ofrecer un esquema de acceso a las actualizaciones de software y firmware disponibles.
- Realizar una jornada de mantenimiento preventivo y los correctivos necesarios durante la vigencia del licenciamiento de la solución, al finalizar cada visita preventiva y/o correctiva el contratista deberá: Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones, y consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración.
- Realizar las actividades requeridas para la correcta ejecución del contrato con personal certificado de la solución de antivirus como implementador, una vez sea suscrita el acta de requerimiento de entrega del contrato el contratista presentará a la Entidad el personal con los soportes que acrediten su idoneidad. Se requieren mínimo dos (2) personas.
- El proponente deberá ser un DISTRIBUIDOR O PARTNER AUTORIZADO POR EL FABRICANTE de la solución ofertada, de modo que se garantice a la Entidad que los interesados en participar dentro del proceso de selección estén autorizados por el fabricante de la solución ofertada para comercializar los bienes y/o servicios requeridos, dado que el contrato comprende actividades que implican el conocimiento en componentes tecnológicos específicos, asimismo, se requiere asegurar que se cuenta con una relación comercial con el fabricante.
- Considerando la calidad de distribuidor autorizado del fabricante, se entiende que el contratista es el enlace y punto de contacto directo entre la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC de la

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

CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

Secretaría General de la Alcaldía Mayor de Bogotá D.C. y el fabricante de la solución, durante la vigencia de la renovación adquirida, y deberá cumplir con todas las políticas establecidas por el fabricante para la ejecución de las actividades requeridas para el cumplimiento del objeto contractual.

4. CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN

- Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista debe garantizar la integridad y confidencialidad de la información institucional a la cual llegue a tener acceso directamente o por intermedio de terceros, para lo cual el contratista suscribe el respectivo compromiso de confidencialidad que hará parte integral del contrato. El contratista deberá asegurar el cuidado, la confidencialidad y la correcta utilización de la información entregada y generada durante la duración de la garantía, soporte y mantenimiento del contrato, así como de los elementos que para su ejecución de la Unidad ponga a su disposición.
- Durante los afinamientos, actualización y soporte de las herramientas, el contratista se compromete a no hacer uso indebido de las herramientas utilizadas en desarrollo del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.

5. EQUIPO DE TRABAJO

PERFIL 1: Líder Técnico Un (01) Ingeniero		
Formación Académica	Profesional	Ingeniería Electrónico o Eléctrico o telemática 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.
	Postgrado	Con especialización o maestría en: Sistemas de Información o Gerencia de Proyectos Informáticos o Telecomunicaciones o Gerencia de Proyectos de Ingeniería o Gestión de Proyectos de Ingeniería o Gerencia de sistemas de información o Gerencia de Proyectos de Telecomunicaciones o seguridad de la información * Certificación vigente como analista y arquitecto de seguridad de redes. Emitida por el fabricante. y/o profesional de seguridad de redes emitida por un fabricante de soluciones de seguridad.
Experiencia	Mínimo cinco (5) años de experiencia relacionada en implementación y/o administración de soluciones de seguridad.	
Roll	Gestionar y articular técnicamente tanto de forma interna como externa, los componentes técnicos de las soluciones ofertadas. Deberá apoyar la revisión de las soluciones, factores de calidad de las implementaciones y supervisión a los procesos en implementación hasta su entrega.	

PERFIL 2: Un (1) Implementador de Seguridad		
Formación Académica	Profesional	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.
	Postgrado o maestría	Con especialización o maestría en: Sistemas de Información o Gerencia de Proyectos Informáticos o Telecomunicaciones o Gerencia de Proyectos de Ingeniería o Gestión de Proyectos de Ingeniería o Gerencia de sistemas de información o Gerencia de Proyectos de Telecomunicaciones o seguridad de la

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

CO18/8583
ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

		información * Certificación vigente como profesional, analista y especialista de seguridad en redes y certificación vigente en arquitecto de seguridad. Emitida por el fabricante.
Experiencia	Mínimo tres (3) años de experiencia relacionada en implementación y/o administración de soluciones de seguridad.	
Roll	Ejecución de las actividades de analista, implementados y documentador de soluciones de TI.	

Nota: El cumplimiento del equipo de trabajo la supervisión realizará la verificación una vez se suscriba el acta de requerimiento de entrega por las partes.

NOTAS GENERALES PARA LA VERIFICACION DEL EQUIPO DE TRABAJO

La experiencia profesional se contabilizará de conformidad con el artículo 229 del Decreto 019 de 2012, esto es a partir de la terminación de materias, por lo que se deberá acreditar con la respectiva certificación expedida por la Institución de Educación Superior, en los casos en que solo se aporte el diploma o acta de grado, esta se tendrá en cuanta a partir de la fecha indicada en estos documentos.

Para el caso de los ingenieros y carreras que estén reguladas por la Ley 842 de 2003 la experiencia empezará a contar a partir de la expedición de la tarjeta y/o matricula profesional.

Los documentos soporte para acreditar por parte del Contratista la experiencia exigida al equipo de trabajo, deberá contener como mínimo la siguiente información:

- Nombre del contratante.
- Valor del contrato (opcional)
- Actividades ejecutadas
- Fecha de inicio del contrato.
- Fecha de terminación del contrato.
- Matrícula profesional vigente para los casos que la ley obligue
- Copia de la tarjeta profesional y registro del COPNIA artículo 6 de la Ley 842 del 2003

Cuando el personal sea certificado por el mismo proponente ya sea de manera individual o como integrante de algún tipo de figura asociativa, debe adjuntar la certificación del contrato de Interventoría que se ejecutó en el cual laboró o prestó sus servicios el profesional; en caso de que el que suscriba la certificación laboral o contractual sea el mismo proponente ya sea por sí mismo o como parte de una estructura plural.

En caso de que el Contratista presente personal extranjero, debe garantizar su presencia en el lugar de ejecución del contrato. Adicionalmente, el Contratista deberá tener en cuenta la legislación vigente y los requerimientos respecto a la contratación de empleados de nacionalidad extranjera, entre otros:

- Exigir la presentación de la visa que le permita desarrollar la actividad, ocupación y oficio autorizado en la misma de conformidad con la legislación vigente que regula la expedición de visas, el ingreso y permanencia de extranjeros al territorio nacional, contenida en el Decreto 834 de 2017, en el Decreto 941 de 2014, Resolución 532 de 2015 y Resolución 6588 de 2013.

- Solicitar la Cédula de Extranjería cuando esté obligado a tramitarla.

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

CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

- Informar por escrito a Migración Colombia sobre la vinculación, contratación o admisión y de su desvinculación o terminación del contrato, dentro de los quince (15) días calendarios siguientes a la iniciación o terminación de labores.

Adicionalmente, el trabajo de extranjeros en Colombia, de acuerdo con lo establecido por el Ministerio de Trabajo, existen algunas profesiones reguladas las cuales requieres de una Matrícula Temporal Especial que otorgan los Consejos profesionales para el ejercicio de la profesión de cada área de conocimiento, en lo referente a la Convalidación de títulos, el procedimiento debe ser realizado por el Ministerio de Educación Superior.

Para cada uno de los profesionales mencionados, se deberá anexar fotocopia de la tarjeta profesional y certificado de vigencia expedido por el consejo profesional competente. El requisito de la tarjeta profesional se puede suplir con el requisito de que trata el artículo 18 del Decreto 2106 de 2019.

Los estudios de posgrado que se exijan como requisito mínimo, se acreditarán mediante copia de los diplomas respectivos o certificado de obtención del título correspondiente. Además, la entidad podrá solicitar las certificaciones laborales que permitan verificar la información relacionada en los Anexos. Para cada uno de los profesionales se debe aportar la información solicitada.

El equipo de apoyo para la ejecución de la interventoría deberá ser definido por el contratista atendiendo a su conocimiento técnico y experticia.

Para el cálculo de la experiencia en años del personal propuesto, se tendrá en cuenta el tiempo efectivo trabajado y no se contabilizarán traslapos por experiencia simultánea, es decir, en caso de traslapos se contabilizará una sola vez dicho periodo.

6. NORMATIVIDAD APLICABLE

- Normas que regulan la contratación estatal en Colombia. (Leyes 80 de 1993 y ley 1150 de 2007) y decretos reglamentarios, Código Civil y Código de Comercio Colombiano.
- Decreto 1078 de 2015 "*por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"* Libro 2, Régimen reglamentario del sector de Tecnologías de la Información y las Comunicaciones, parte 1 Disposiciones Generales Titulo 1 Objeto y ámbito de aplicación.
- Ley 1340 de 2009 "*por medio de la cual se dictan normas en materia de protección de la competencia".*
- 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.

7. OBLIGACIONES DEL CONTRATISTA:

7.1. Obligaciones especificas

1. Cumplir con todas las especificaciones técnicas definidas por la Entidad.
2. Suscribir el acta de requerimiento de entrega dentro de los tres (3) días siguientes al cumplimiento de requisitos y perfeccionamiento del contrato.

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

CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

3. Suministrar dentro de los cinco (5) días hábiles posteriores a la firma del acta de requerimiento de entrega del contrato, el cronograma de donde se contemple todas las actividades necesarias para el desarrollo del objeto contractual, y se apruebe por parte de la Supervisión del contrato.
4. Entregar el licenciamiento de acuerdo con las especificaciones técnicas solicitadas por la Entidad.
5. Entregar documento expedido por el fabricante donde conste la titularidad y vigencia de la adquisición, en el sitio indicado por la entidad, en la ciudad de Bogotá D.C.
6. El contratista deberá realizar la Instalación, Implementación, configuración, afinamiento y puesta en marcha de la solución de Antivirus adquirido y deberá dejar el producto operando correctamente.
7. Prestar soporte técnico en el momento que sea requerido por la Secretaría General de la Alcaldía Mayor de Bogotá D.C., por medio del supervisor del contrato y/o apoyo a la supervisión que será informado una vez se inicie la Ejecución del contrato.
8. Acatar las instrucciones que durante el desarrollo del contrato se le impartan por parte de la de la Secretaría General de la Alcaldía Mayor de Bogotá D.C por medio del supervisor del contrato y/o apoyo a la supervisión que será informado una vez se inicie la Ejecución del contrato.
9. Realizar los respectivos informes de cada una de las sesiones de soporte o afinamiento de la herramienta adquirida, que deben ser entregada dentro de los tres (3) días hábiles siguientes a la realización de la actividad.
10. El contratista debe cumplir con la política de seguridad de la información y privacidad de los datos de la Entidad, así como con los requerimientos del SGSI (Sistema de Gestión de Seguridad de la Información) de la Secretaría General de la Alcaldía Mayor de Bogotá.
11. Asumir todos los costos que genere la legalización del presente contrato.
12. Informar por escrito (carta, correo electrónico o acta suscrita con el supervisor) respecto a la cantidad de personas que participaran en la ejecución contractual, una vez sea suscrita el acta de inicio. Con el propósito de verificar la aplicabilidad del Decreto No. 332 de 2020

7.2. Obligaciones generales

1. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y trabas que puedan presentarse y en general se obliga a cumplir con lo establecido en la Ley 80 de 1993, Ley 1150 de 2007 y sus Decretos Reglamentarios.
2. No acceder a peticiones o amenazas de quienes actúen por fuera de la ley con el fin de hacer u omitir algún hecho.
3. Responder ante las autoridades de los actos u omisiones en el ejercicio de las actividades que desarrolle en virtud del contrato que se celebre, cuando con ellos cause perjuicio a la Administración.
4. Constituir y mantener vigente a favor del "Distrito Capital - Secretaría General de la Alcaldía Mayor de Bogotá, D.C., una garantía única en las condiciones establecidas en la invitación pública.
5. Realizar los actos necesarios y tomar las medidas conducentes para el debido y oportuno cumplimiento de las obligaciones contractuales y la ejecución del contrato.
6. Asumir el pago de los impuestos, gravámenes, aportes parafiscales y servicios de cualquier género que establezcan las leyes colombianas.
7. Acatar las instrucciones que durante el desarrollo del contrato se le impartan por parte de la Secretaría General a través del Supervisor del contrato.
8. Responder ante las autoridades de los actos u omisiones que en el ejercicio de las actividades se desarrollen, cuando con ellos se cause perjuicio a LA SECRETARÍA GENERAL o a terceros.
9. Tener una cuenta corriente o de ahorros en una entidad bancaria afiliada al S.A.P. (Sistema Automático de Pagos).
10. Asumir todos los costos que genere la legalización del presente contrato.

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

CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

11. Dar cumplimiento a las normas de conservación y protección del medio ambiente, de conformidad con lo dispuesto en Directiva 006 del 30 de octubre de 2012, modificada por la Directiva Nro. 002 de 2014, en relación con el manejo del medio ambiente de la Secretaría General de la Alcaldía Mayor de Bogotá DC.
12. Mantener estricta reserva y confidencialidad sobre la información que conozca por causa o con ocasión del contrato.
13. Velar por el respeto de los Derechos Constitucionales y Laborales de los trabajadores que utilice para la ejecución del contrato, para lo cual, eliminará formas de contratación lesiva para los Derechos Laborales.
14. Las demás obligaciones que se desprendan de la naturaleza del contrato.
15. Cumplir con las normas reglamentos e instrucciones de Sistema de gestión de Seguridad y Salud en el trabajo.

7.3. Obligaciones ambientales

1. Entregar los informes y la documentación relacionada con la ejecución del contrato de manera digital en cumplimiento de la política cero papel de la Secretaría General con código 4233100-OT-079. Informes y/o soportes de la ejecución del contrato. De acuerdo con la periodicidad establecida en el proceso.

8. PLAZO DE EJECUCIÓN

El plazo para la ejecución del contrato será de dos (2) meses, contados a partir de la fecha de suscripción del acta de requerimiento de entrega, previo cumplimiento de los requisitos de perfeccionamiento y ejecución.

9. LUGAR DE EJECUCIÓN

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

10. FORMA DE PAGO DEL VALOR DEL CONTRATO

La Secretaría General de la Alcaldía Mayor de Bogotá D.C realizará un único pago del 100% del valor del contrato, una vez se verifique la instalación, configuración, puesta en funcionamiento, y la entrega de los documentos soporte de las actividades realizadas y que acrediten la titularidad de la solución a nombre de la Entidad; previa presentación de la factura y soportes por parte del contratista, y una vez se expida la certificación del recibo a satisfacción suscrita por el supervisor del contrato.

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 el(os) proponente(s) favorecido(s) en el presente proceso de selección y bajo ningún motivo o circunstancia efectuará pagos a terceros.

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

SYSTEM CERTIFICATION ISO 9001 SGS CO18/8583

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

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 proponente seleccionado, 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).
NOTA 7: El CONTRATISTA asumirá la totalidad de los gastos que se originen en relación con el objeto del contrato; al igual que los porcentajes por concepto de Impuestos, tasas y/o contribuciones se calcularán, de conformidad con las disposiciones que rijan la materia.

11. PROTOCOLO DE BIOSEGURIDAD

De requerirse actividades en sitio, se deberá dar cumplimiento a las actividades que fomenten el autocuidado en las instalaciones de la Entidad, para lo cual se debe tener en cuenta las siguientes recomendaciones.

- Garantizar que se cumplan todas las medidas de higiene y de distanciamiento referidas en el numeral 4.1. de la Resolución 666 de 2020 expedida por el Ministerio de Salud y Protección Social, además de desarrollar un proceso diario de monitoreo del estado de salud antes de iniciar las actividades.
- Verifique que cuenta con los documentos de afiliación al sistema de seguridad social integral (EPS, AFP, ARL).
- Dar cumplimiento con el protocolo establecido por la Empresa contratante para desarrollar la labor, el cual deberá socializarse y armonizarse con el Protocolo de la Secretaria General de la Alcaldía Mayor de Bogotá, D.C.
- No se permitirá el ingreso o acompañamiento a las instalaciones, de personas que presenten síntomas de gripa, cuadros de fiebre mayor o igual a 38°C o síntomas de afección respiratoria. En todo caso, cuando se presente esta situación deberá reportarse de forma inmediata a la Dirección de Talento Humano.

➢ **Durante el desarrollo de actividades:**

- Promover el reporte de incidentes, realizar el reporte de accidentes de trabajo.
- Garantizar el cumplimiento específico para casos sospechosos o confirmados de COVID19.
- Investigar todos los incidentes y accidentes de trabajo e implementar los planes de acción.

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

CO18/8583
ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

ROBERTO DÍAZGRANADOS DÍAZ
Jefe Oficina de Tecnologías de la Información y las Comunicaciones
Oficina de Tecnologías de la Información y las Comunicaciones

Elaboro: Jhon Fernando Rincon Sánchez
Reviso: Wilson Hortua Ramos

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

CO18/8583

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA GENERAL