Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	SOLICITUD DE BIENES Y SERVICIOS	CÓDIGO: AP-CT-F-75-01
		VERSIÓN: 1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA CONTRATACIÓN	PÁGINA: 1 DE 1
		FECHA: 18/07/2023

Numero del Plan Anual		Valor del plan		150.000.000	

1.Bogotá DC. 18/09/2025

2. INFORMACIÓN

2.1. La solicitud está incluida en el Plan de adquisiciones: Si: X No:

2.2. Justificación de la necesidad:

La Subred Integrada de Servicios de Salud Norte E.S.E., fue creada en el marco de la reorganización del sector salud en el Distrito Capital en cumplimiento de lo dispuesto en el artículo 2 del Acuerdo 641 de abril 6 de 2016, expedido por el Honorable Concejo de Bogotá D.C, mediante el cual se reorganiza el sector salud del Distrito Capital el cual dispuso: fusionar las siguientes Empresas Sociales del Estado, adscritas a la Secretaría Distrital de Salud de Bogotá, D.C., como sigue: (...) Empresas Sociales del Estado de Engativá, Simón Bolívar, Suba, Usaquén, Chapinero se fusionan en la Empresa Social del Estado denominada "Subred Integrada de Servicios de Salud Norte E.S.E."

De conformidad con el artículo 2. Naturaleza Jurídica contenida en los Estatutos , es una Entidad Pública de categoría especial, descentralizada, dotada de personería jurídica, patrimonio propio y autonomía administrativa, cuyo objeto es la prestación del servicio público de salud a cargo del Estado, por lo que tiene a su cargo acciones de promoción, prevención, diagnóstico, tratamiento y rehabilitación de la salud, ejecutando planes, programas, proyectos y actividades de investigación y docencia, observando los principios de igualdad, solidaridad y rentabilidad social.
Derivado de lo anterior, esta Subred presta servicios de salud de baja, mediana y alta complejidad adelantando acciones de promoción de la salud y prevención de la enfermedad a nivel individual y colectivo para brindar atención integral, con altos estándares de calidad y eficiencia, en cumplimiento de las normas vigentes de habilitación y acreditación, contribuyendo al desarrollo social y la mejora en la calidad de vida, la morbilidad, la mortalidad, la incapacidad física o secuelas que puedan conllevar en la población usuaria y sus familias.

Con el propósito de satisfacer sus requerimientos y necesidades, esta E.S.E., debe adelantar procesos de adquisición de bienes y/o servicios, todos los cuales se rigen por normas de Derecho Privado, conforme lo dispuesto en los artículos 194, 195 numeral 6 y 197, de la Ley 100 de 1993; el Código Civil; el Código de Comercio; sus Estatutos y Manual de Contratación vigentes y le asiste la facultad de, discrecionalmente, utilizar las cláusulas exorbitantes previstas en el Estatuto General de Contratación de la Administración Pública.

Sin perjuicio de lo anterior, el artículo 13 de la Ley 1150 de 2007, establece que las Entidades que por disposición legal cuenten con un régimen contractual distinto al General de Contratación de la Administración Pública, aplicarán, en desarrollo de su actividad contractual y acorde con su régimen legal especial, los principios de la función administrativa y de la gestión fiscal de que tratan los Artículos 209 y 267 de la Constitución Política, según sea el caso y estarán sometidos al régimen de inhabilidades e incompatibilidades previstos legalmente para la contratación estatal.
}
De acuerdo con el régimen de Derecho Privado de la Entidad establecido desde el numeral 6 del artículo 195 de la ley 100 de 1993, y, dado que la invitación a cotizar pertenece a una de las modalidades de contratación directa de la Entidad, las estipulaciones y el contenido del presente documento, como en general el proceso de contratación, no obligan ni tampoco comprometen a la Entidad a realizar una adjudicación y en cualquier momento puede ocurrir su terminación anticipada.

Es importante resaltar que, disponer oportunamente de los insumos requeridos para el apoyo en la prestación de los servicios de salud, da cumplimiento a los estándares del Sistema Único de Habilitación establecidos en la Resolución 3100 de 2019, que define "los procedimientos y las condiciones de inscripción de los prestadores de servicios de salud y de habilitación de los servicios de salud" y adopta el "Manual de Inscripción de Prestadores y Habilitación de Servicios de Salud". Lo anterior siempre que, la norma señala expresamente que, para el funcionamiento de los servicios de salud que cualquier tipo de prestador, se deben garantizar las condiciones mínimas, allí establecidas, para proteger y asegurar a los usuarios.

Actualmente, la Subred opera con una plataforma tecnológica que incluye múltiples sistemas de información, servidores y estaciones de trabajo que deben estar protegidos contra amenazas como virus, troyanos, ransomware, spyware y demás software malicioso. En promedio, se generan más de 1.000 nuevas amenazas mensuales, lo que exige contar con un sistema antivirus corporativo de última generación que garantice detección temprana, protección en tiempo real y respuesta automatizada frente a incidentes de seguridad.

La seguridad de la información se encuentra alineada con el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001, así como con las exigencias del Decreto 2693 de 2012 en materia de protección de la confidencialidad, integridad y disponibilidad de los activos de información.

Se requiere la adquisición de 2.500 licencias de solución de seguridad avanzada (on-premise o nube) con despliegue centralizado desde una consola de administración, sin intervención manual en cada equipo. La solución debe incluir protección EDR, control de dispositivos, firewall de host, sandboxing, análisis de reputación de archivos, protección multiplataforma y reportes personalizados. El servicio debe incluir soporte 7x24, mantenimiento, actualizaciones automáticas y capacitación al personal técnico.

La implementación abarcará todas las sedes y dependencias de la Subred Norte E.S.E., incluyendo aproximadamente 40 servidores y 2.460 estaciones de trabajo, distribuidos en áreas administrativas y asistenciales, con el fin de asegurando la continuidad operativa y la actualización permanente de las bases de datos de amenazas.

No contar con esta protección generaría un alto riesgo para la seguridad de la información institucional, afectando la prestación de servicios misionales y administrativos, pudiendo ocasionar: pérdida o secuestro de información, interrupción de servicios críticos, saturación de canales de red y degradación de rendimiento, incumplimiento de normativas en seguridad y protección de datos personales.

2.3. Área solicitante:

Oficina Sistemas de Información - TIC

09:48
24/09/25
→Johana
- Natalia

3. CARACTERISTICAS DEL BIEN O SERVICIO A CONTRATAR

3.1. Descripción del objeto:

ADQUISICIÓN DEL LICENCIAMIENTO SOFTWARE DE SEGURIDAD ANTIVIRUS PARA LOS EQUIPOS DE LA SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E

3.2 Garantías a constituir por el oferente:

PÓLIZA CUMPLIMIENTO DEL CONTRATO (X)
En los contratos cuya cuantía naturaleza o complejidad así lo exija, el contratista deberá constituir esta garantía, para precaver los perjuicios que se deriven del incumplimiento de las obligaciones contractuales, independiente de las multas y la cláusula penal que se pacte en el contrato. Su cuantía corresponderá a la que en cada caso se determine, la cual no podrá ser inferior al diez por ciento (10%) del monto del contrato y una duración igual a la del plazo máximo previsto al momento de la suscripción del contrato y cuatro (4) meses más.

3.3. Plazo del contrato u orden:	Tres (3) meses
3.4. Plazo de entrega:	Dos (2) meses

3.5. Lugar y forma de entrega de los bienes o de la prestación:

Almacén General de la Subred Norte ESE, ubicado en la sede Fray Bartolome de las Casas Av Suba #106-47

3.6. Especificaciones técnicas e información de referencia

Descripción:		Ver anexo técnico 1
Presentación:		Licencia
Cantidad:		2500
Materiales:		N/A
Dimensiones:		N/A
Otros:		N/A

3.7. Valoración de los riesgos previsibles:

Se anexa formato AP-CT-F-02-Análisis de riesgos

4.ESPECÌFICACIONES DEL BIEN O SERVICIO REQUERIDO

Suministro de licencia antivirus para 2.500 equipos, solución de seguridad avanzada (on-premise o nube) para estaciones de trabajo y servidores.
Versión: La última versión liberada por el fabricante a la fecha de inicio del contrato, compatible con el idioma del sistema operativo donde se instalará la solución.
Administración: Consola local de administración centralizada, con alta disponibilidad, balanceo y cifrado TLS 1.3.
Protección de Nueva Generación: Motor antimalware, Machine Learning, HIPS, análisis de comportamiento y bloqueo de exploits. Protección avanzada contra amenazas 0-day mediante sandboxing en la nube.
EDR: Plataforma de monitoreo en tiempo real, caza de amenazas y respuesta automatizada a incidentes.
Control de Dispositivos: Bloqueo granular de dispositivos como USB, Bluetooth, impresoras, cámaras y Wi-Fi, configurable por usuario, grupo o ubicación.
Cobertura de Protocolos: Inspección de protocolos HTTP/HTTPS, SMTP/IMAP/POP3, FTP/SFTP, SMB y WebDAV.
Mantenimiento: Soporte 7×24 en español e inglés. Severidad 1: respuesta ≤ 1 hora y restauración ≤ 4 horas. Incluye actualizaciones de módulos y versiones durante 12 meses.
Capacitación: Capacitación certificada de 16 horas (8 h de administración y 8 h de nivel avanzado), incluyendo entrenamiento en herramientas de detección de amenazas, automatización y reportes.
Actualización: Suscripción a la base de datos por un periodo de un (1) año.
Soporte de Idioma: Soporte mínimo para español e inglés.
Aplicación de Políticas por Grupos: Agrupación de agentes en grupos para facilitar configuración y administración.
Detección y Prevención: Funciones de detección y prevención de intrusos a nivel de host en estaciones y servidores.
Notificaciones de Ataques: Alertas ante ataques con notificación a administradores por eventos críticos vía e-mail.
Protección en Aplicaciones de Mensajería: Detección, análisis y neutralización de virus propagados por aplicaciones de mensajería y carpetas compartidas.
Análisis de Reputación de Archivos: Capacidad de evaluar la reputación de archivos.
Protección en Tiempo Real: Análisis y desinfección de archivos, programas, páginas web, correos electrónicos, discos y memorias USB en tiempo real, bloqueando archivos sospechosos.
Firewall de Host: Centralización de políticas desde consola, programación de validez de reglas, creación de reglas por aplicación y definición de zonas de confianza para ciertas IP, protocolos o aplicaciones.
Análisis por Demanda: Ejecución remota de búsquedas, detección y eliminación de amenazas.
Control de Aplicaciones: Vista de riesgo de aplicaciones en endpoints y reducción de privilegios sin afectar su funcionalidad.
Aislamiento de Aplicaciones: Reducción del riesgo y exposición mediante aislamiento.
Integración con Correo Electrónico: Agentes para sistemas de correo con antispam y análisis de adjuntos.
Control de Dispositivos Avanzado: Gestión de dispositivos infrarrojos, firewire, PCMCIA, puertos serie y paralelo, con permisos/bloqueos por "ID de Clase" e "ID de Dispositivo".
Integración con Directorio Activo: Conexión y sincronización para administración y control centralizados.
Protección de Directorio Activo: Defensa contra escalada de privilegios y movimiento lateral en entornos AD.
Condiciones del Antivirus: Verificación de firmas y del servicio activo.
Condiciones de Archivos: Comprobación de existencia, antigüedad, tamaño y versión de archivos.
Condiciones de Parches: Verificación de Service Pack y parches instalados.
Condiciones de Registro: Validación de existencia de llaves, establecimiento de valores y verificación de registros.

Condiciones de Utilidad: Comprobación de servicios y procesos en ejecución.
Configuración de Políticas: Adaptación de políticas a usuarios o grupos específicos.
Reportes: Generación de informes personalizables (virus detectados, estaciones infectadas, versiones instaladas, etc.).
Escalabilidad: Actualización automática para 2.500 máquinas, sin intervención del usuario.
Repositorios Distribuidos: Administración de repositorios que optimicen carga y distribución.
Cuarentena e Informe: Almacenamiento de archivos sospechosos en cuarentena para análisis/restauración.
Instalación/Desinstalación: Instalación y desinstalación remota desde consola.

5. PÉRFIL Y NOMBRE DE QUIEN EJERCERÁ LA SUPERVISIÓN

1. Nombre:	VICTOR JULIO GOMEZ CARVAJAL
2. Identificación:	91281972
3. Perfil	JEFE OFICINA SISTEMAS DE INFORMACION - TIC

6. RECURSOS

Recursos Propios: SI [X] NO [ ] Vigencias Futuras: SI [ ] NO [X]

Convenio: SI [ ] NO [ ] No. Convenio: _____ Suscrito con: _____

7.(FIRMA DEL SOLICITANTE)
Victor Julio Gómez Carvajal
Jefe Oficina Sistemas

8. VoBo. (NOMBRE Y FIRMA)
Victor Julio Gómez Carvajal
Director -Jefe de Oficina

9. Control y VoBo Verificación Presupuestal Subgerencia Corporativa: Ing. Rafael Guillermo Ochoa Ortiz **10. FECHA:** _____

11. Fecha de Recepción en la Dirección de Contratación : _____

