SECRETARÍA DISTRITAL DE SALUD FONDO FINANCIERO DISTRITAL DE SALUD
ANEXO TÉCNICO

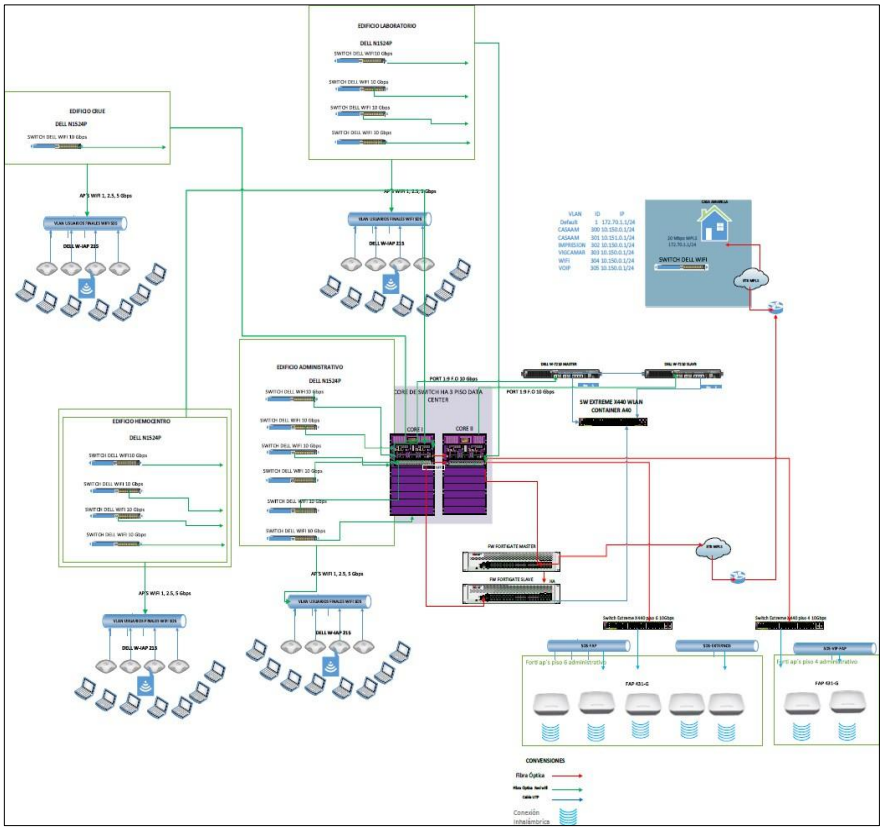
Objeto: Adquirir la plataforma WIFI para la secretaria Distrital de Salud.

Alcance del Objeto: Adquirir una plataforma de red wifi instalada, configurada y puesta en operación de acuerdo con la topología de red inalámbrica que defina la entidad, con los componentes indicados y las condiciones técnicas dadas en el documento de Anexo Técnico, para garantizar el servicio de conectividad inalámbrica de la entidad.

1. Topología de red inalámbrica.

Actualmente la entidad cuenta con una topología de red inalámbrica implementada, con cobertura en sus instalaciones.

Imagen 1 *Topología de la Red Actual*



Basados en la topología actual un análisis de estudio en sitio (Site Survey) y considerando obsolescencia y vida útil de los equipos que la conforman, desde la Dirección TIC se han definido los

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

componentes requeridos para la solución de cobertura de red inalámbrica en las instalaciones de la entidad y como resultado se estima que sea conformada por los siguientes elementos requeridos para su implementación, administración centralizada y gestión; Access Point, Switches Poe. Dicha topología se debe instalar en las instalaciones de la SDS las cuales se describen a continuación:

EL EDIFICIO ADMINISTRATIVO:

Consta de siete (7) pisos, cuya distribución está de la siguiente manera: en el primer piso se encuentran los auditorios, la oficina de seguridad, recepción, correspondencia y atención al usuario, el centro de cableado se ubica aproximadamente en la mitad de los dos costados y distribuye la red vertical de cables al sótano, primer y segundo piso; en el segundo piso se encuentra la biblioteca y la cafetería; en los pisos 3, 4, 5, 6 y 7 presentan una distribución de puestos de trabajo en costado oriental y costado occidental, el centro de cableado se ubica aproximadamente en la mitad de los dos costados.

EDIFICIO HEMOCENTRO:

Cuarto (4) pisos; en el primer piso al costado sur se encuentra un área de laboratorios y al costado norte está el almacén del Hemocentro.
En el segundo piso al costado sur están ubicados unas áreas de consultorios, un salón de charlas y dos oficinas, al costado sur se ubican una sala de espera, el área de donación de sangre y tres consultorios.
El tercer piso presenta una distribución de puestos de trabajo en costado sur y costado norte.
En el cuarto piso al costado sur se ubica el auditorio alterno, y hay un área de oficinas, al costado norte se ubican oficinas de trabajo.
En los cuatro pisos el centro de cableado se ubica aproximadamente en la mitad de los dos costados.

EDIFICIO HEMOCENTRO BAJO:

Primer (1) piso consiste en un corredor que al lado y lado se encuentra áreas de laboratorio y de oficinas administrativas de los laboratorios.
El centro de cableado se ubica aproximadamente en la mitad del corredor.

EDIFICIO LABORATORIO:

Cuatro (4) pisos; en el primer y segundo piso son dos corredores que al lado sur y norte se encuentran áreas de laboratorio y aproximadamente hacia la mitad de los corredores hay una oficina.
El tercer piso hacia el costado oriental hay dos oficinas separadas por un corredor, en el centro del piso hay otra oficina al lado de la recepción y en el costado occidental hay una oficina en donde se distribuyen puestos de trabajo.
En el cuarto piso presentan una distribución de puestos de trabajo en costado oriental y occidental.
En el cuatro piso el centro de cableado se ubica aproximadamente en la mitad de los dos costados.

EDIFICIO CRUE O DUES:

Siete (7) pisos, es un edificio de un área pequeña de una dimensión aproximada de 10*10 en el primer piso esta la recepción y hay dos oficinas.

En el segundo piso hay un salón de asesorías y eventos de información a ciudadanos.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

En el tercer piso hacia el costado oriental hay una sala de radio y a su vez en este espacio se encuentra el centro de cableado de datos del edificio, al costado occidental hay una oficina de emergencias y desastres.

En el cuarto piso está el centro regulador de urgencias y se encuentra el call center de la atención de urgencias.

En el quinto piso está ubicada una sala de administración del centro regulador de urgencias.
En el sexto piso esta la dirección del CRUE y hay un área de distribución de puestos de trabajo.
En el séptimo piso está ubicada una sala de crisis y hay una distribución de puestos de trabajo.

SEDE REMOTA:
Dos Pisos, es un edificio ubicado en la Calle 13 # 31-96.
En el primer piso se encuentra un área abierta de trabajo y archivo.
En el segundo piso hay un área abierta de trabajo.

PLAZOLETA CENTRAL Y TERRAZAS DE EDIFICIOS ADMINISTRATIVO, HEMOCENTRO, LABORATORIO:
A la salida de cada uno de los edificios de la SDS se encuentra una plazoleta central que en ocasiones es usada para eventos de diversa índole, se requiere garantizar la conectividad en estas áreas.
La SDS cuenta con aproximadamente 2.267 funcionarios y para este proyecto de red Wi-Fi se considera una población flotante de 400 personas. Todos los usuarios tendrán acceso a internet.

2. Códigos Del Clasificador De Bienes Y Servicios- Unspsc

Tabla 1 *Códigos Del Clasificador De Bienes Y Servicios- Unspsc*

SEGMENTO	FAMILIA	CLASE	PRODUCTO
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	**43220000** Equipos o plataformas y accesorios de redes multimedia o de voz y datos	**43221700** Equipo fijo de red y componentes	**43221721** Equipo de comunicación de información por radiofrecuencia.
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	**43220000** Equipos o plataformas y accesorios de redes multimedia o de voz y datos	**43222500** Equipo de seguridad de red	**43222500** Equipo de seguridad de red.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

SEGMENTO	FAMILIA	CLASE	PRODUCTO
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	**43220000** Equipos o plataformas y accesorios de redes multimedia o de voz y datos	**43222600** Equipo de servicio de red.	**43222600** Equipo de servicio de red.
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	**43220000** Equipos o plataformas y accesorios de redes multimedia o de voz y datos	**43222600** Equipo de servicio de red.	**43222631** Estaciones base de fidelidad inalámbricas.
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	**43220000** Equipos o plataformas y accesorios de redes multimedia o de voz y datos	**43222600** Equipo de servicio de red.	**43222633** Adaptadores de manejo remoto.
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	**43220000** Equipos o plataformas y accesorios de redes multimedia o de voz y datos	**43222600** Equipo de servicio de red.	**43222634** Dispositivo de monitoreo o manejo de redes.
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	**43220000** Equipos o plataformas y accesorios de redes multimedia o de voz y datos	**43222600** Equipo de servicio de red.	**43222640** Punto de acceso inalámbrico.
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	**43220000** Equipos o plataformas y accesorios de redes multimedia o de voz y datos	**43222800** Equipo de telefonía	**43222814** Kits de instalación o modificación de equipos de telecomunicaciones.
810000000 Servicios Basados en Ingeniería, Investigación y Tecnología	**81110000** Servicios informáticos	**81111700** Sistemas de manejo de información MIS	**81111702** Diseño de comunicaciones por redes de área local.
810000000 Servicios Basados en	**81110000** Servicios informáticos	**81111800** Servicios de sistemas y	**81111803** Mantenimiento o

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

SEGMENTO	FAMILIA	CLASE	PRODUCTO
Ingeniería, Investigación y Tecnología		administración de componentes de sistemas	soporte de redes de área local (LAN).
810000000 Servicios Basados en Ingeniería, Investigación y Tecnología	**81110000** Servicios informáticos	**81111800** Servicios de sistemas y administración de componentes de sistemas	**81111809** Servicio de instalación de sistemas.
810000000 Servicios Basados en Ingeniería, Investigación y Tecnología	**81110000** Servicios informáticos	**81111800** Servicios de sistemas y administración de componentes de sistemas	**81111818** Garantía de terceros.
810000000 Servicios Basados en Ingeniería, Investigación y Tecnología	**81110000** Servicios informáticos	**81111800** Servicios de sistemas y administración de componentes de sistemas	**81111819** Servicios de garantía de calidad.

3. Características Técnicas Mínimas.

En virtud del objeto contractual se requiere para EL FONDO FINANCIERO DISTRITAL DE SALUD - SECRETARÍA DISTRITAL DE SALUD, que la solución tecnológica debe satisfacer los siguientes componentes y sus características:

Tabla 2 *Características técnicas*

ITEM	COMPONENTE	CANTIDAD
1	• Las controladoras deben instalarse y configurarse en entornos On-Premise; soportar políticas RBAC, VLANs, QoS, servicios IoT (identificación o localización de activos). • Cada controladora debe tener minino dos (2) fuentes de energía en alta disponibilidad. • Las controladoras deben incluir administración centralizada con capacidades de monitoreo en tiempo real, tales como calidad de conexiones por frecuencia (2.4/5/6 GHz), velocidad, canales e interferencias; estado de APs, usuarios autenticados por SSID, throughput y dispositivos clasificados por sistema operativo; análisis de tráfico (top aplicaciones consumidoras) y diagnóstico de fallos integrado. • Las controladoras deben soportar autenticación IEEE 802.1X con Radius/ AAA y métodos EAP-TLS, PEAP y WPA3,	2

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

ITEM	COMPONENTE	CANTIDAD
	integrándose con directorios LDAP/Active Directory, además permitir la asignación dinámica de políticas basadas en roles. • La plataforma de gestión debe permitir configurar reglas basadas en roles para filtrar tráfico por IP, puerto, aplicación o usuario, integrándose con políticas de segmentación de red. Las ACL deben soportar priorización QoS, restricciones de acceso según tipo de dispositivo y detección de tráfico anómalo, con capacidad de actualización dinámica según cambios en la topología o políticas de seguridad. • La plataforma de gestión debe integrar e incluir herramientas o módulos avanzados de análisis RF, planificación de redes, tales como mapas dinámicos en tiempo real para optimizar cobertura, densidad de usuarios y asignación de canales. Estas funciones deben generar informes detallados de interferencias, calidad de señal (SNR, RSSI), compatible con bandas 2.4 GHz, 5 GHz y 6 GHz. • La plataforma de gestión debe integrar e incluir herramientas o módulos avanzados de AIOPs para analizar los datos de telemetría de la red cableada e inalámbrica, para establecer umbrales adaptativos de SLA para las métricas de LAN, actualizando dinámicamente los valores de referencia de latencia, fluctuación, pérdida de paquetes y rendimiento de redes cableadas e inalámbricas, e identificar desviaciones significativas respecto al comportamiento normal. Se debe obtener Triaje y debe ofrecer recomendaciones para resolver problemas en la red LAN, incluyendo cambios de configuración y acciones como prueba de cables (permitir verificación del rendimiento de la infraestructura de cableado). • La plataforma de gestión debe tener la capacidad de centralizar e integrar de forma nativa, conector o vía API, la gestión de diez (10) Access Point FortiAP 431F con los que cuenta actualmente la entidad. • La plataforma de gestión debe tener integración con la plataforma centralizada de registros y reportes FortiAnalyzer 1000G de la entidad, para centralizar los logs de las plataformas de seguridad, red LAN y WLAN, para tener visibilidad y estandarización en reportería, análisis más detallado y control automatizado: La solución deberá integrarse nativamente, a través de conectores, API o mecanismos estándar con la plataforma centralizada de Logs y reportes de la Entidad para recolección, normalización,	

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

ITEM	COMPONENTE	CANTIDAD
	almacenamiento, análisis y generación de reportes a partir de registros (logs). • La plataforma de gestión debe soportar integración nativa o API con herramientas tipo Sandbox, que permita el envío automático de archivos sospechosos identificados en el tráfico de red hacia un entorno de ejecución controlado para su análisis dinámico, habilitando la detección de amenazas de día cero y comportamientos maliciosos no identificados por firmas tradicionales. Asimismo, la solución debe ser capaz de recibir y aplicar de forma automática los resultados del análisis (indicadores de compromiso), reforzando las políticas de seguridad en tiempo real tanto para el tráfico cableado como inalámbrico gestionado. Esta capacidad permitirá a la Entidad fortalecer la protección integral de la red de acceso, reducir el riesgo de propagación de malware avanzado y mejorar la visibilidad y respuesta frente a incidentes de seguridad en entornos distribuidos. • La solución debe ser nueva, no remanufacturada y se pueden utilizar herramientas tecnológicas con las que cuenta actualmente la Entidad.	
2	**Access Point Indoor (entornos internos)** • Estos elementos deben ser del mismo fabricante de las controladoras para garantizar compatibilidades y óptimo funcionamiento. • Los Access Point debe soportar los estándares IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax, (Wi-Fi 6E), y 802.11be (Wi-Fi 7), 4K- QAM, y canales de 320 MHz. Además, debe cumplir con estándares de gestión de red (802.11k/r/v), seguridad (802.11i), y calidad de servicio (802.11e). • Los AP´s debe ser compatible con estándares IEEE 802.3at (PoE+), 802.3bt (Ultra PoE) y opcional alimentación directa de CC (12V/3A). En modo PoE, debe consumir máximo 42 W. • Los AP´s debe operar simultáneamente en tres bandas (2.4 GHz, 5 GHz y 6 GHz), con capacidades de transmisión combinadas que alcancen mínimo 18 Gbps de velocidad agregada (mínimo 1.1 Gbps en 2.4 GHz, 5.5 Gbps en 5 GHz y 11.5 Gbps en 6 GHz). • Los AP´s deben soportar mínimo 500 usuarios por radio en sus tres bandas (2.4 GHz, 5 GHz y 6 GHz), para un total de	108

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

ITEM	COMPONENTE	CANTIDAD
	1500 usuarios. • Los AP´s deben permitir configuración de hasta 8 SSIDs por radio en sus tres bandas e integración con políticas de segmentación VLAN para redes corporativas, visitantes y dispositivos IoT. • Los AP´s debe incorporar tecnologías MIMO 4x4 en cada banda (2.4 GHz, 5 GHz y 6 GHz) y compatibilidad con MU-MIMO. Debe contar con una arquitectura de antenas optimizada con mínimo 4 antenas dual band para 2,4GHz /5Ghz, así como antenas de una banda para 6 Ghz, y sensores IoT o BLE, para garantizar cobertura y rendimiento en entornos de alta densidad. • Los AP´s debe incluir escaneo de radios que permitan el monitoreo continuo de interferencias no autorizadas y análisis de espectro. • Contar con dos puertos ethernet: 100M/1000M/2500M/5000M/10000 Mbps Multigigabit Ethertnet RJ45. • Las antenas internas deben ofrecer una ganancia mínima de 4.0 dBi en 2.4 GHz, 5.4 dBi en 5 GHz, 5.2 dBi en 6Ghz, con diseño optimizado para reducir interferencias y mejorar la cobertura. • Disponer de una potencia de transmisión de por lo menos 23 dBm o dB para 2.4GHz, 23 dBm o dB para 5GHz y 23 dBm o dB para 6GHz. • Soportar los siguientes estándares de seguridad: WPA, WPA2, y WPA3 con 802.1x o Preshared key, WEP, Web Captive Portal, MAC blacklist y whitelist. • Soporte OFDMA, Spatial Reuse (BSS Coloring), UL MU-MIMO, DL MU-MIMO, Enhanced Target Wake Time (TWT), ZeroWait DFS y Cellular Co-existence. • Debe soportar los siguientes estándares IEEE: 802.11a, 802.11b, 802.11be, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax, 802.11mc, 802.1X, 802.3ad, 802.3at, 802.3bt, 802.3az, 802.1Q, 802.11u, 802.11w, 802.3bz • Modos de radio Rogue Scan mínimo soportado: Background y dedicado • Modos de radio WIPS / WIDS mínimo soportado: Background y dedicado. • Los AP´s ofertados debe contar con certificación Wifi 7 por la Wifi Alliance adjuntado documento certificado.	

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

ITEM	COMPONENTE	CANTIDAD
	• Los APs deben soportar mínimo FCC y/o RoHS • La solución debe integrarse nativamente, vía conector, API o sistema estándar a las soluciones de seguridad y SIEM, con los que cuenta la entidad. • La solución debe integrarse con la herramienta de Logs y Reportes de la entidad para tener visibilidad y estandarización en reportería: Los puntos de acceso inalámbrico ofrecidos y/o la controladora deberán integrarse a través de conectores, API o mecanismos estándar con la plataforma centralizada de Logs y reportes de la Entidad para recolección, normalización, almacenamiento, análisis y generación de reportes a partir de registros (logs). Dicha integración deberá permitir la visibilidad operacional y de desempeño de la infraestructura inalámbrica, soportando el envío de eventos, métricas y alarmas relacionados con disponibilidad, utilización, autenticación, calidad de servicio y experiencia del usuario, así como la generación de reportes históricos, dashboards operativos y análisis detallado para soporte, auditoría y toma de decisiones. Como mínimo se deben desplegar reportes de disponibilidad y estado, tráfico y rendimiento, eventos operativos, rendimiento y calidad de la red inalámbrica, radiofrecuencia (RF), seguridad y operaciones inalámbricas.	
3	**Access Point Outdoor (entornos externos)** • Estos elementos deben ser del mismo fabricante de los Access Point Indoor para garantizar compatibilidades y óptimo funcionamiento. • Los Access Point debe soportar los estándares IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax, (Wi-Fi 6E), y 802.11be (Wi-Fi 7), 4K- QAM, y canales de 320 MHz. Además, debe cumplir con estándares de gestión de red (802.11k/r/v), seguridad (802.11i), y calidad de servicio (802.11e). • Los AP´s debe operar simultáneamente en tres bandas (2.4 GHz, 5 GHz y 6 GHz), con capacidades de transmisión combinadas que alcancen mínimo 10,5 Gbps de velocidad agregada (680 Mbps en 2.4 GHz, 4,3 Gbps en 5 GHz y 5.6 Gbps en 6 GHz). • Disponer de una potencia de transmisión de por lo menos 20 dBm o dB para 2.4GHz, 20 dBm o dB para 5GHz y 20 dBm o dB para 6GHz.	8

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

ITEM	COMPONENTE	CANTIDAD
	• Los AP´s debe ser compatible con estándares IEEE 802.3at (PoE+), 802.3bt (Ultra PoE) y opcional alimentación directa de CC (12V/3A). En modo PoE, debe consumir máximo 28 W. • Los AP´s deben permitir configuración de hasta 8 SSIDs por radio en sus tres bandas e integración con políticas de segmentación VLAN para redes corporativas, visitantes y dispositivos IoT. • Los AP´s debe incorporar tecnologías MIMO 2x2 en cada banda, compatibilidad con UL MU-MIMO y DL MU-MIMO. Debe contar con sensores IoT o BLE. • Soportar los siguientes estándares de seguridad: WPA, WPA2, y WPA3 con 802.1x o Preshared key, WEP, Web Captive Portal, MAC blacklist y whitelist. • Debe soportar mínimo los siguientes tipos de EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPV0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST, EAP-TTLS/PAP. • Los APs deben tener mínimo una interfaz 1x RJ-45 Multi-Gigabit Ethernet (100 M / 1 G / 2.5 G / 5 G), 802.3bt PoE IN. • Las antenas deben ofrecer una ganancia mínima de 6 dBi en 2.4 GHz, 9.2 dBi en 5 GHz, 8.2 dBi en 6Ghz. • Los AP´s debe incluir escaneo de radios que permitan el monitoreo continuo de interferencias no autorizadas y análisis de espectro. • Deben ser modelos resistentes a condiciones climáticas externas como mínimo IP67. • Los APs deben soportar Enhanced Target Wake Time (TWT). • Modos de radio Rogue Scan mínimo soportado: Background y dedicado • Modos de radio WIPS / WIDS mínimo soportado: Background y dedicado. • Los AP´s ofertados debe contar con certificación Wifi 7 por la Wifi Alliance. • Los APs deben soportar mínimo FCC, IC y CE • Mean Time Between Failures (MTBF) > 10 años • La solución debe integrarse nativamente, vía conector, API o sistema estándar a las soluciones de seguridad y SIEM, con los que cuenta la entidad. • La solución debe integrarse con la herramienta de Logs y	

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

ITEM	COMPONENTE	CANTIDAD
	Reportes de la entidad para tener visibilidad y estandarización en reportería: Los puntos de acceso inalámbrico y/o la controladora ofrecidos deberán integrarse a través de conectores, API o mecanismos estándar con la plataforma centralizada de Logs y reportes de la Entidad para recolección, normalización, almacenamiento, análisis y generación de reportes a partir de registros (logs). Dicha integración deberá permitir la visibilidad operacional y de desempeño de la infraestructura inalámbrica, soportando el envío de eventos, métricas y alarmas relacionados con disponibilidad, utilización, autenticación, calidad de servicio y experiencia del usuario, así como la generación de reportes históricos, dashboards operativos y análisis detallado para soporte, auditoría y toma de decisiones. Como mínimo se deben desplegar reportes de disponibilidad y estado, tráfico y rendimiento, eventos operativos, rendimiento y calidad de la red inalámbrica, radiofrecuencia (RF), seguridad y operaciones inalámbricas.	
4	**Switch de 24 puertos RJ45** • Estos elementos deben ser del mismo fabricante de los Access Point y garantizar compatibilidades y óptimo funcionamiento con las controladoras y los Access Point. • Debe contar con veinticuatro (24) puertos 1/2.5/5 GbE RJ45, cumpliendo el estándar IEEE 802.3af/at/bt con soporte para PoE de mínimo 90W por puerto. Presupuesto de energía PoE mínimo de 1440W. • Los switches deben incluir mínimo cuatro (4) módulos 1/10/25 Gigabit Ethernet auto negociables SFP/SFP+/SFP28 con su respectiva licencia compatibles con los Switch de distribución y los switches Core instalados en la secretaria Distrital de Salud. • Debe incluir un puerto 10/100/1000 dedicado para gestión o administración fuera de banda. • Debe permitir integración transparente en gestión centralizada, segmentación VLAN y servicios de automatización. • Debe soportar estándares como IEEE 802.3bz (Multi-Gig Ethernet), 802.3b o 25GbE, y 802.3bt (PoE++) • Deben tener la capacidad de administración, que incluyan las herramientas para configurar, hacer seguimiento, monitoreo y administración completa de la infraestructura de equipos	17

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

ITEM	COMPONENTE	CANTIDAD
	activos adquiridos. • Los switches deben incluir fuentes de alimentación AC redundantes (mínimo dos por switch), diseñados para operación en caliente (hot-swap). Cada fuente de poder del Switch debe soportar mínimo 1000W de potencia para carga PoE. • Cada switch debe tener un throughput mínimo de 440 Gbps y un Forwarding rate de 650 Mpps. • Cada switch debe incluir: Un (1) puerto de consola serial RJ45 o puerto USB. • Protocolos de gestión segura (HTTPS, SSH, SNMPv3) y compatibilidad con sistemas de monitoreo externos. • Los switches deben ser tipo rack (1U) • Debe tener latencia <1µs • Vlan soportadas: Mínimo 4.000 • Almacenamiento de dirección MAC mínimo: 64.000 • Packet Buffer de mínimo: 8 MB • Temperatura de funcionamiento como mínimo entre: 0°C to 45°C • Mean Time Between Failures (MTBF) > 10 años • Debe integrarse nativamente, con conectores, vía API, o incluir una solución de orquestación con las soluciones de seguridad, Firewall de Nueva Generación, Logs y reportes con los que cuenta la entidad. • Integración con plataforma centralizada de registros y reportes de la entidad para tener visibilidad y estandarización en reportería: Los switches ofrecidos deberán integrarse a través de conectores, API o mecanismos estándar con la plataforma centralizada de Logs y reportes de la Entidad para recolección, normalización, almacenamiento, análisis y generación de reportes a partir de registros (logs). Dicha integración deberá permitir la visibilidad operacional y de desempeño de la infraestructura cableada, soportando el envío de eventos, métricas y alarmas relacionados con disponibilidad, utilización, errores de puertos, autenticación, calidad de servicio y experiencia del usuario, así como la generación de reportes históricos, dashboards operativos y análisis detallado para soporte, auditoría y toma de decisiones. Como mínimo se deben desplegar reportes de disponibilidad y estado, puertos e interfaces, tráfico y rendimiento y eventos operativos. • El switch deberá soportar Control de acceso basado en roles	

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

ITEM	COMPONENTE	CANTIDAD
	y tipo de dispositivo • Debe estar en la capacidad de detectar Dispositivos IoT. • Segmentación dinámica por identidad • Microsegmentación a nivel de Puerto • Aprovisionamiento remoto y seguro • Capacidad de aplicar políticas de tráfico definidas centralmente • El Switch debe permitir descargar políticas de seguridad desde el Firewall perimetral de la Entidad • La solución debe incluir funcionalidades Network Access Control (NAC) básicas integradas en la solución o con licenciamiento adicional (pe: Identificación automática de dispositivos conectados a puertos de acceso, asignación dinámica de políticas de acceso, cuarentena automática de dispositivos comprometidos, etc) y capacidad de integrarse con soluciones de NAC externas de propósito específico a través de protocolos estándar. • La solución debe incluir funcionalidades avanzadas de seguridad y gestión de red, soporte protocolos de árbol de expansión como IEEE 802.1D MAC Bridging/STP, 802.1w RSTP, 802.1s MSTP, además de asignación de VLAN dinámica. Debe cumplir con estándares como los RFC 2474 (definición de DS Field), RFC 1157, RFC 2865 y RFC 2866. Entre las medidas de seguridad se requieren STP root guard, STP BPDU guard, Storm control, Per-port Storm control, Loop guard, IGMP snooping, IGMP proxy. En términos de QoS, debe permitir priorización de tráfico mediante IEEE 802.1p incluyendo Priority Queuing y WRED, QoS queue counters, Tail-drop policy, WRED drop policy, QoS Marking (IPv4/IPv6), Real-time egress queue rates. Adicionalmente, debe integrar el estándar IEEE 802.1X asignación dinámica de VLANs y DHCP Snooping.	

4. REQUISITOS TÉCNICOS DE INTEGRACION

La solución WIFI deberá garantizar la integración y compatibilidad con los Access Point FortiAP actualmente instalados en la Entidad, los cuales hacen parte de la infraestructura tecnológica existente y se encuentran integrados al ecosistema de seguridad institucional bajo el concepto de ***Fortinet Security Fabric*** (plataforma de malla de ciberseguridad y arquitectura integrada de Fortinet). Esta integración es necesaria para preservar la inversión tecnológica realizada, garantizar la continuidad de los servicios de conectividad inalámbrica y mantener la gestión, visibilidad, monitoreo y aplicación coordinada de políticas de seguridad sobre la infraestructura de red.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

La adquisición de Access Point (AP) con capacidades de seguridad integradas del fabricante Fortinet tiene como finalidad fortalecer la protección de la infraestructura de comunicaciones inalámbricas de la entidad, frente a posibles amenazas y ataques de seguridad que puedan originarse a través de conexiones maliciosas por medio de los de Access Point (AP).

En consideración a que los Access Point (AP) constituyen elementos de conectividad que permiten el acceso de dispositivos a la red institucional y cuya protección no debe depender exclusivamente de las configuraciones de seguridad implementadas en los switches de acceso, se requiere que los equipos incorporen mecanismos de seguridad propios y que, adicionalmente, permitan su integración con el ecosistema de seguridad implementado en la Entidad.

Esta integración deberá facilitar la aplicación centralizada de políticas de seguridad, monitoreo, identificación y control de dispositivos, así como la detección y gestión de eventos de seguridad, contribuyendo al establecimiento de un perímetro de seguridad de red más robusto, que permita fortalecer la protección de la infraestructura tecnológica y reducir los riesgos asociados al acceso inalámbrico a la red institucional.

Tabla 3 Requisitos técnicos de integración

ITEM	REQUERIMIENTO TECNICO MINIMO DE OBLIGATORIO CUMPLIMIENTO
1	Integración nativa con el ecosistema Security Fabric, ya que la entidad cuenta actualmente con un firewall Fortigate 1101E, FortiClient ZTNA y Fortianalyzer. La solución de WIFI debe integrarse de forma nativa o API con la plataforma de seguridad perimetral existente para que los Firewalls actuen como controlador central de la red, permitiendo la gestión unificada de los switches y la aplicación de políticas de acceso basadas en identidad. Integración nativa con el ecosistema Security Fabric, ya que la entidad cuenta actualmente con un firewall Fortigate 1101E, FortiClient ZTNA y Fortianalyzer. La solución de WIFIdebe integrarse de forma nativa o API con la plataforma de seguridad perimetral existente para que los Firewalls actúen como controlador central de la red, permitiendo la gestión unificada de los switches y la aplicación de políticas de acceso basadas en identidad. La solución de WIFI debe integrarse de forma nativa o API con la plataforma Forticlient ZTNA, para lo cual debe soportar la utilización de etiquetas dinámicas de acceso seguro (ZTNA tags) originadas en la solución ZTNA existente en la entidad, de tal manera que dichas etiquetas puedan ser consumidas por el controlador central de los Switches (Firewall) para definir y aplicar políticas de segmentación y control de acceso a nivel de puerto de red, VLAN o equivalentes, en los Switches a adquirir. La solución de WIFI debe integrarse de forma nativa o API con la herramienta de Logs y reportes FortiAnalyzer existente, de modo que los Switches gestionados centralmente por los Firewall envíen sus eventos e información de operación de manera directa o indirecta,

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

ITEM	REQUERIMIENTO TECNICO MINIMO DE OBLIGATORIO CUMPLIMIENTO
	permitiendo su consolidación, correlación y análisis. En este esquema, los eventos de red, cambios de configuración, autenticación y actividad de usuarios en los WIFI deben ser visibles desde el FortiAnalyzer, asegurando trazabilidad unificada y capacidades de auditoría sobre el entorno de acceso cableado. Cuando la integración de la solución de WIFI con el ecosistema Security Fabric de la entidad se realice mediante API el fabricante deberá garantizar, implementar, soportar y mantener la interoperabilidad de la solución propuesta con los Firewall, Logs y eventos y ZTNA actualmente implementados por la entidad. Para tal efecto el oferente deberá presentar certificación emitida por el fabricante o su representante autorizado en Colombia, firmada por el representante legal, donde conste dicho compromiso. La solución de Switching debe integrarse de forma nativa o API con la plataforma Forticlient ZTNA, para lo cual debe soportar la utilización de etiquetas dinámicas de acceso seguro (ZTNA tags) originadas en la solución ZTNA existente en la entidad, de tal manera que dichas etiquetas puedan ser consumidas por el controlador central de los Switches (Firewall) para definir y aplicar políticas de segmentación y control de acceso a nivel de puerto de red, VLAN o equivalentes, en los Switches a adquirir. La solución de WIFI debe integrarse de forma nativa o API con la herramienta de Logs y reportes FortiAnalyzer existente, de modo que los Switches gestionados centralmente por los Firewall envíen sus eventos e información de operación de manera directa o indirecta, permitiendo su consolidación, correlación y análisis. En este esquema, los eventos de red, cambios de configuración, autenticación y actividad de usuarios en los switches deben ser visibles desde el FortiAnalyzer, asegurando trazabilidad unificada y capacidades de auditoría sobre el entorno de acceso cableado. Cuando la integración de la solución de WIFI con el ecosistema Security Fabric Y FORTINEC de la entidad se realice mediante API el fabricante deberá garantizar, implementar, soportar y mantener la interoperabilidad de la solución propuesta con los Firewall, Logs y eventos y ZTNA actualmente implementados por la entidad. Para tal efecto el oferente deberá presentar certificación emitida por el fabricante o su representante autorizado en Colombia, firmada por el representante legal, donde conste dicho compromiso.

5. Condiciones Técnicas Mínimas

La solución tecnológica que se entrega para brindar cobertura de red inalámbrica, objeto de esta contratación, debe cumplir las siguientes condiciones técnicas mínimas:

5.1. Garantía.

La solución tecnológica de red inalámbrica debe ser instalada, configurada y entregada en operación, con los soportes (físico o digital), a nombre de la secretaria Distrital de Salud, expedido por el

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

fabricante donde se describa registro de licenciamiento, soporte y garantía por Dos (2) años directo con fábrica a partir del recibido a satisfacción de los equipos por parte de la supervisión, sobre todos los bienes adquiridos descritos en el presente documento, verificable en la página web del fabricante. Los equipos deben ser nuevos y no remanufacturados.

5.2. Licenciamiento.

Los componentes, el software para el funcionamiento de la plataforma de wifi, y la plataforma de gestión, deberán estar licenciados a perpetuidad para funcionalidades de gestión de la solución de Access Point y Switches.

El software necesario para el funcionamiento de la plataforma de wifi, y la plataforma de gestión, deben ser actualizados cada vez que el fabricante libere nuevas versiones compatibles, durante la vigencia del soporte garantía.

5.3. Soporte Técnico de la garantía de los equipos.

Se detallan las condiciones del soporte técnico y los tiempos de respuesta que deben ser cumplidos en función de la clasificación de los incidentes y las solicitudes, los cuales se regirán por los principios de transparencia, eficiencia y buena fe, que rigen el marco normativo de la contratación pública. En caso de vacíos o situaciones no contempladas en este documento, se deberán aplicar las normas ITIL como estándar de buenas prácticas para la gestión de servicios tecnológicos.

Se debe brindar soporte técnico con el fabricante sobre todos los bienes adquiridos (hardware y software) descritos en el presente documento, durante la vigencia del soporte y garantía.

El soporte entregado debe realizarse a través de un único canal certificado que garantice trazabilidad, tiempo de respuesta 7x24x365, durante la vigencia del soporte y garantía.

Las actualizaciones del software necesario para el funcionamiento de la plataforma de wifi, y la herramienta de administración y monitoreo, deben incluir parches de seguridad, correcciones críticas y compatibilidad con nuevos estándares.

Los componentes que requieran ser reemplazados por garantía debe seguir el procedimiento de control de registro de inventarios del almacén de la entidad y sin costos para la entidad.

El contratista, se compromete a entregar un procedimiento en el cual se proporcione un número telefónico y un e-mail disponible durante el tiempo acordado para brindar atención de llamadas 7x24 de consultas técnicas, reportes de fallas, creación de Tickets de soporte y seguimiento de estos.

5.3.1. Soporte remoto

El contratista deberá brindar diagnóstico remoto de la causa del incidente y la validación de la posibilidad de la solución vía remota. También le indicará a la persona designada por la Secretaría Distrital de Salud, las posibles acciones requeridas. Luego de alcanzar la solución al inconveniente reportado esta se corroborará mediante un chequeo de funcionamiento, y luego de esto de la Secretaría Distrital de Salud debe autorizar el cierre del caso.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

5.3.2. Soporte técnico vía web

El contratista, deberá contar con un software para el manejo de Tickets a través de su página WEB. Por medio de este sistema y con las autorizaciones necesarias para el personal de la Secretaría Distrital de Salud asignado, para crear y tener un control sobre sus tickets abiertos y cerrados. Además, contar con los permisos y accesos a la base de conocimientos, que pueda servir, de ayuda para la solución de un caso actual.

5.3.3. Soporte vía email

El contratista, se compromete a proporcionar un e-mail de contacto a través del cual personal autorizado por de la Secretaría Distrital de Salud podrá requerir los servicios de atención de fallas, consultas sobre el estado de los ticket e información relacionada con el objeto de estos.
La Secretaría Distrital de Salud a través del Supervisor o el personal encargado delegarán con nombre, correo electrónico, teléfono, al encargado de tratar asuntos relacionados con el presente contrato y recibir los informes que se generen y, a este se reportarán los soportes establecidos por los mecanismos descritos, su avance y su cierre.

5.3.4. Soporte telefónico

El contratista, se compromete a proporcionar un número telefónico y un e-mail disponible durante el tiempo acordado para brindar atención de llamadas 7x24 de consultas técnicas, reportes de fallas y seguimiento de estas.
El Soporte Técnico Telefónico no tiene un límite de llamadas y se debe prestar en un horario 7x24.

5.3.5. Soporte técnico en sitio

El contratista, deberá ofrecer el servicio de soporte técnico en sitio por el tiempo requerido y hasta definir una solución al caso, para ello el contratista dispondrá de un ingeniero de soporte en las instalaciones de la entidad, disponible para el diagnóstico y resolución de fallas durante el tiempo requerido.

5.3.6. Tiempos de respuesta

El registro de cualquier incidencia se puede realizar 7x24 en el portal web, herramienta de gestión, vía correo electrónico, vía telefónica, sin embargo, para los casos de atención en sitio, el horario de atención 5x8.

Los tiempos de respuesta de acuerdo con la clasificación del incidente registrado son los siguientes:

Tabla 4 *Tiempos de respuesta*

NIVEL DE SEVERIDAD	TIEMPO DE RESPUESTA TELEFONICO/REMOTO PARA DIAGNÓSTICO	TIEMPO DE RESPUESTA EN SITIO
S1	30 MINUTOS	Ingeniero en sitio antes de 4 horas, contado a partir del reporte de la falla, atención 7*24*365

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

NIVEL DE SEVERIDAD	TIEMPO DE RESPUESTA TELEFONICO/REMOTO PARA DIAGNÓSTICO	TIEMPO DE RESPUESTA EN SITIO
S2	MENOS DE 60 MINUTOS	Ingeniero en sitio antes de 6 horas, contado a partir del reporte de la falla, atención 7*24*365
S3	MENOS DE CUATRO HORAS	Visita programada dentro de las siguientes ocho (8) horas hábiles, contado a partir del reporte de la falla para el siguiente horario: L-V de 7:00am a 5:00 pm S de 7:00 am a 1:00pm
S4	SIGUIENTES OCHO HORAS HABILES ANTES DE 24 HORAS HABILES	Visita programada dentro de las siguientes veinticuatro (24) horas hábiles, contado a partir del reporte de la falla para el siguiente horario: L-V de 7:00am a 5:00 pm S de 7:00 am a 1:00pm

5.3.7. Tiempo de aplicación de garantías.

El contratista se compromete a aplicar las garantías y dar solución a incidentes y requerimientos en un lapso no mayor a 48 horas. En caso de ser necesario el retiro o suspensión de algún componente de la solución adquirida por más de 48 horas, el contratista debe suministrar un componente reemplazo que garantice el servicio de conectividad de manera temporal mientras se reemplaza el componente afectado, los componentes entregados en reemplazo (temporal o definitivo) deben cumplir con las mismas o mejores características ofertadas.

Nota: Cuando un remplazo sea definitivo, este no deberá ser remanufacturado y debe ser nuevo.

5.4. Implementación de la solución.

Los componentes de la solución deben incluir funcionalidades IA y automatización como aprendizaje, razonamiento, percepción, comprensión de lenguaje, análisis de datos, automatización, el tiempo de vida (end of life - EOL) de los componentes es de mínimo cinco (5) años.

El contratista debe suministrar e instalar los puntos de red de datos necesarios en áreas internas y externas donde se requiera brindar cobertura de red inalámbrica, incluyendo jack, face plate, patch panel, patch cord y demás elementos necesarios para la conectividad de los Access point, garantizando la certificación categoría 6ª del cableado. La ubicación de estos puntos de red está sujeta a las necesidades de la entidad.

Los puntos de red nuevos a instalar en áreas internas deben ser certificados y cumplir con las normas

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

vigentes de cableado estructurado ANSI/TIA-568-C.0 y C.1, TIA/EIA–569, TIA/EIA–606 y la ISO/IEC 11801, además de la norma colombiana NTC 2050. Los puntos de red nuevos a instalar en áreas externas deben ser certificados y cumplir con las normas vigentes de cableado estructurado para exteriores ANSI/TIA-568-D, ANSI/TIA-569-D, ANSI/TIA-758-B, RETIE y la ISO/IEC 11801, además de la norma colombiana NTC 2050.

El contratista deberá realizar la certificación del cableado UTP existente de la solución inalámbrica, desde patch panel hacia ubicación de Access Point; y en caso de identificar fallos en el cableado, el proveedor realizará el cambio de este sin ningún costo para la entidad. En todo caso se debe garantizar la certificación categoría 6ª e instalación de los elementos de red necesarios para su correcto funcionamiento.

El contratista debe suministrar los cables de potencia, patch cord de FO, patch cord red LAN, software, licencias, transceivers, y demás elementos físicos, lógicos y técnicos (cables, rieles, tornillería y demás elementos que se requieran) necesarios para su instalación, configuración e integración, de tal manera que todos los insumos necesarios sean entregados por el contratista como parte integral de la instalación, así no estén solicitados de forma específica.

El contratista debe garantizar cobertura inalámbrica con la misma solución para la sede remota Calle 13 # 31-96, suministrando los equipos necesarios para esta comunicación que permita el uso y consumo de los mismos servicios entre la sede principal y la sede remota.

El contratista debe realizar el desmonte y entrega de los elementos de la infraestructura actual que se van a retirar y que quedarán fuera de servicio, para su reintegro al almacén de la entidad, acompañado del inventario de estos elementos para la verificación y aprobación de parte de la supervisión.

5.5. Plan de trabajo.

El contratista debe presentar un plan de trabajo con cronograma de actividades, de obligatorio cumplimiento para su ejecución, previa aprobación por parte de la supervisión, que incluya el diseño, instalación, configuración, parametrización, pruebas de operación y servicio, puesta en funcionamiento, transferencia de conocimiento, documentación técnica e informe de implementación, finalización con el recibido a satisfacción por parte de la supervisión, y demás actividades para el cumplimiento del objeto y alcance del contrato, detallando para cada actividad fechas y tiempo de ejecución discriminado en semanas, personal responsable designado, hitos, secuencia y ruta crítica.

EL plan de trabajo deberá ajustarse al plazo de ejecución del contrato.

5.6. Diseño de la solución.

Se debe realizar el diagrama de implementación teniendo en cuenta la configuración de la plataforma de gestión que incluye controladoras en alta disponibilidad, la disminución de puntos de fallo, el mayor desempeño de red y la seguridad; incorporando las mejores prácticas del fabricante, de redes y de seguridad.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

El contratista concertar con el supervisor el diagrama de implementación propuesto por la entidad, para realizar los ajustes requeridos para la implementación.

5.7. Instalación.

La instalación, configuración y puesta en operación de la solución adquirida, debe incluir su integración con la infraestructura de Red LAN actual de la entidad, de conformidad con las características técnicas de la red instalada en la entidad.
Se debe realizar la configuración del software, hardware y firmware a la última versión estable aprobada por el fabricante.

La instalación de la solución se debe realizar de acuerdo con las mejores prácticas de los fabricantes, se deben realizar pruebas de operación y servicio.

5.8. Transferencia de conocimiento.

Realizar la transferencia de conocimiento, con una duración de un (1) día hábil previa instalación, sobre la plataforma Wi-Fi, que incluya los procedimientos de instalación, configuración y administración básica de los dispositivos adquiridos.

5.9. Documentación técnica e informe de implementación.

El contratista debe adjuntar los folletos, catálogos u hojas de especificaciones técnicas de los productos, soporte y garantía ofrecidos.

El contratista debe entregar en medio digital un informe detallado del diseño, instalación, pruebas, certificaciones, licenciamientos, configuraciones y parametrización de cada una de las funcionalidades implementadas, con los respectivos soportes y guías de usuario en español o traducías al español, aprobado por la supervisión del contrato.

5.10. Entrega de la solución.

El contratista debe asumir todos los costos o gastos asociados a la logística (desplazamiento, transporte, equipos y herramientas de trabajo, entre otros) requerida para el cumplimiento del objeto y alcance del contrato por parte del personal asignado al proyecto.

5.11. Certificaciones.

Los Switches y Access Point del presente proceso deben ser nuevos y no remanufacturados, deben tener garantía, con Servicio directo de fábrica 7x24, actualización de firmware y/o software, que incluya Soporte Telefónico y repuestos.

La solución debe integrarse nativamente a la plataforma de seguridad, Firewalls, SIEM, Logs y reportes que posee actualmente la entidad, para control y aplicación de políticas de seguridad y visibilidad. el fabricante de la solución de Access Point y Switches deberá garantizar, implementar, soportar y mantener la interoperabilidad de la solución propuesta con las herramientas actualmente implementadas por la entidad.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

5.12. Equipo de trabajo y experiencia específica.

El contratista debe presentar las hojas de vida y las respetivas certificaciones del grupo de trabajo asignado para realizar la implementación, expedidas por los fabricantes de los componentes ofertados.

5.12.1. Gerente de proyecto.

Un (01) Ingeniero Gerente de Proyecto

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines.
● Posgrado en Gerencia de Proyectos y/o Certificación PMP vigente.
● Certificación vigente en ITIL Foundation v3 o superior.

Experiencia mínima de cinco (5) proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática. Tarjeta Profesional con expedición mínima de diez (10) años.

5.12.2. Ingeniero de Líder Técnico.

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.
● Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad.
● Certificación vigente en SCRUM Foundations Professional (SFPC).
● Certificación vigente como especialista en seguridad en redes. Emitida por el fabricante con el cual se esté presentado el proponente.
Experiencia general de mínimo ocho (8) años a partir de la expedición de la tarjeta profesional. La experiencia se cuenta a partir de la expedición de la tarjeta profesional

5.12.3. Ingeniero Implementador

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.

● Certificación vigente como profesional de seguridad en redes
● Certificación vigente como especialista en seguridad en redes

Experiencia general de mínimo cinco (5) años a partir de la expedición de la tarjeta profesional. La experiencia se cuenta a partir de la expedición de la tarjeta profesional

5.12.4. Ingeniero de Soporte

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.
● Certificación vigente como profesional de seguridad en redes
● Certificación vigente como especialista en seguridad en redes
Experiencia general de mínimo cinco (5) años a partir de la expedición de la tarjeta profesional. La experiencia se cuenta a partir de la expedición de la tarjeta profesional

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

5.12.5. Técnico de instalación

Dedicación 100 % Técnico de instalación de AP, con Certificado de curso de alturas y cableado estructurado, para la implementación de los AP interiores y exteriores.

Elaborado: Arnold Julián / Contratista SDS

Arnol Julian Martinez P.
CC 1587664

Firmado digitalmente por Arnol Julian Martinez Paredes

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.