ANEXO TÉCNICO

1. OBJETO

Adquirir componentes de conectividad de la red LAN para la actualización tecnológica de los sistemas de comunicaciones de red de la secretaria distrital de salud.

2. ALCANCE DEL OBJETO

Entregar los equipos que conforman la solución de conectividad de la red LAN, correspondientes a switches de acceso y de distribución, junto con su respectivo licenciamiento, así como los conectores SFP (transceivers) necesarios para su correcto funcionamiento, de acuerdo con las condiciones técnicas establecidas en el Anexo Técnico.

El contratista debe realizar la instalación, configuración, parametrización, integración y puesta en funcionamiento de la solución e integración, con los demás sistemas de comunicaciones y con las soluciones perimetrales existentes dentro del modelo de Security Fabric, y su puesta en operación de acuerdo con la topología actual de red implementada en la Entidad. Esta implementación deberá permitir el servicio de conectividad de la red LAN de la entidad, incluida la sede ubicada en la Calle 13 #31-96.

3. SOLUCIONES PARA SUMINISTRAR

3.1. REQUISITOS TÉCNICOS DE SWITCH DE ACCESO 48 PUERTOS

ITEM	REQUERIMIENTO TECNICO MINIMO DE OBLIGATORIO CUMPLIMIENTO
1	Suministro de Ochenta y dos (82) switches de acceso capa 2.
2	Arquitectura de gestión centralizada
3	Integración con plataformas de ciberseguridad de la Entidad
4	Capacidades de monitoreo, analítica y optimización operativa
5	Soporte técnico y garantía por 24 meses
6	**Arquitectura y Factor de forma** • Factor de forma 1RU, montaje en rack estándar de 19” • Fuente de poder redundante • MTBF mínimo esperado: ≥ 10 años • Soporte como mínimo de certificaciones FCC, CE, RCM, VCCI y RoHS2 • Garantía limitada de por vida directo con el fabricante (5 años después del fin de venta)
7	**Interfaces y Conectividad (mínimo requerido)** El switch ofertado deberá contar como mínimo con:

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
	• 48 puertos Ethernet RJ45 de acceso 10M/100M/1G/ (auto-negociables) • 4 puertos de uplink 10 Gigabit Ethernet (compatibles SFP+/SFP) • Puerto de consola serial RJ 45 o USB • Puerto dedicado de gestión
8	**Capacidades de Conmutación** • Capacidad de switching (full duplex): ≥ 176 Gbps • Reenvío de paquetes (pps): ≥ 262 Mpps • Latencia máxima: ≤ 1 µs • Tabla MAC: mínimo 32.000 direcciones • VLANs soportadas: mínimo 4.000 **Administración:** • Interfaz de línea de Comandos Estándar de la Industria, SNMP V1/2c/3 • Administración de VLAN, Soporte a Voice VLAN. • Soportar administración basada en SSH y telnet. • Soportar OpenFlow o Netconf o Rest APIs. • Soportar SFlow o Netflow. • Debe soporta administración desde sistemas de gestión en nube o on-premise • En caso de no contarse con el Controlador SD-LAN, este debe incluirse en la propuesta con todas las funcionalidades y sistema de gestión necesarias para este proyecto. Se debe poder administrar Switches, Access Point, SD-WAN y Firewalls desde la misma consola de Administración.
9	**Funcionalidades de Capa 2** • Soportar RMON (RFC 2819), Sflow (RFC 3176) • IEEE 802.1Q. VLAN IDs >= 4.000. Soportar IEEE 802.1ad QinQ • Private VLAN • Soporte de egregación de enlaces L2 vía LACP • Mínimo ACLs 1.000 • Entrada de Host minimo 2.000 • Soportar DHCPv6 snooping, IPv6 RA guard • debe contar con IPV6 nativo y homologado por el fabricante (Certificado de fábrica) y se debe soportar la activación del Dual stack. • Debe contar con al menos un medio de monitoreo o alerta de fallas en conexiones de cobre, y un medio de monitoreo de fallas en conexiones de fibra. Especificar la nomenclatura del fabricante de estos métodos tanto para conexiones de cobre como para conexiones de fibra. • STP root guard, STP, RSTP, MSTP • Debe soportar MCLAG (multi chassis aggregation) • QoS que cumpla con: Clasificación, marcado, policy, strict priority, WRED

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
	• Debe soportar Egress priority Mapping (IPv4/IPv6) • Packet buffer mínimo 4 MB • Debe soportar notificación de congestión explícita (ECN) para IPv4 e IPv6
10	**Seguridad Integrada en la Red de Acceso** **El switch deberá soportar:** • Control de acceso basado en roles 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 • Debe soportar el movimiento de clientes de un puerto a otro sin necesidad de borrar la sesión 802.1X • El switch debe permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad • Debe permitir la autenticación y autorización Local RADIUS y TACAS+ • Debe soportar DHCP snooping, IP source guard, Dynamic ARP • Debe soportar IEEE 802.1X (Port Based Network Access Control) • Debe soportar PTP (IPv4 e IPv6) • El Switch debe permitir descargar políticas de seguridad desde el Firewall perimetral de la Entidad • 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

11	**Gestión Centralizada de los Switches de acceso**
	
	Los Switches de acceso deben ser gestionados desde una plataforma (Controladora SD-LAN) del mismo fabricante de los Switches o sobre plataformas con las que cuente la Entidad en la actualidad y que permitan:
	
	• Administración completa desde una única consola en Appliance físico.
	• Definición centralizada de:
	  ○ VLANs
	  ○ Políticas de acceso
	  ○ Segmentación de red
	  ○ Prioridades de tráfico
	• Eliminación de la gestión individual por dispositivo
	• Aplicación automática de políticas de seguridad en la capa de acceso
	• Soporte de Zero Touch Provisioning y aprovisionamiento remoto seguro

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
	• Descubrimiento automático de Switches Los Switches deben integrarse nativamente o via API a los Firewall referencia FG-1101E que posee actualmente la entidad, para gestión centralizado, control unificado de tráfico, control y aplicación de políticas de seguridad y visibilidad. Cuando la integración se realice mediante API el fabricante deberá garantizar, implementar, soportar y mantener la interoperabilidad de la solución propuesta con los Firewall actualmente implementados por la entidad. Para tal efecto el contratista deberá presentar certificación emitida por el fabricante o su representante autorizado en Colombia, firmada por el representante legal, donde conste dicho compromiso. La plataforma de gestión debe tener integración con la plataforma centralizada de registros y reportes FortiAnalyzer 300F y FortiAnalyzer 1000G de la entidad, para centralizar los logs de las plataformas de seguridad, red LAN, 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, 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, eventos operativos. 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.
12	**Generalidades de los Switches de Acceso** • Suministrar los cables de potencia, patchcord de FO, patchcord red LAN, conectores, tarjetas, software, licencias, transceivers, y demás elementos físicos, lógicos y técnicos (cables, rieles, tornillería y demás elementos que se requieran) necesarios para su configuración e instalación, de tal manera que todos los insumos necesarios sean

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
	entregados por el contratista como parte integra, así no estén solicitados de forma específica. • Soporte para apilamiento, apilamiento virtual o gestión de múltiples switches. Deben ser incluidos los cables necesarios (mínimo un cable por Switch) y con una longitud mínima de 3 metros. • La plataforma deber contar con la capacidad de integración nativa con herramientas de Digital Experience Monitoring (DEM) del mismo fabricante, facilitando futuras estrategias de visibilidad y monitoreo de la experiencia del usuario final. • Administración de los Switches: o Interfaz de línea de Comandos Estándar de la Industria, SNMP V1/2c o 3 o Soportar ACL o Administración de VLAN, Soporte de Voice VLAN o similar o Soportar administración basada en SSH y telnet. o Soportar OpenFlow o Netconf o Rest APIs. o Administración mediante consola para CLI (Command Line Interface). No se admiten equipos de línea Small Business: Equipos cuya administración sea únicamente a través de htttp/https. • Capacidad de escalar como mínimo a 196 de Switches bajo la misma plataforma central de gestión. • Gestión, Monitoreo y Auditoría de los Switches de Acceso y Distribución o Registro de eventos centralizado o Trazabilidad de cambios o Exportación de logs • Se debe garantizar y proveer licenciamiento/servicios necesarios para la integración con plataformas y herramientas con las que cuenta actualmente la Entidad, través de protocolos estándar, conectores o vía API con: o Plataforma de analítica y reportes o Plataformas de seguridad existentes • Suministrar los cables de potencia, patchcord de FO, patchcord red LAN, conectores, tarjetas, software, licencias, transceivers, y demás elementos físicos, lógicos y técnicos (cables, rieles, tornillería y demás elementos que se requieran) necesarios para su configuración e instalación, 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. • Brindar soporte y garantia de dos (2) años para todo el hardware y servicios entregados en funcionamiento, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la página web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. • Brindar licenciamiento de la infraestructura y software contratado de dos (2) años, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la página

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
	web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. • Brindar garantía de la infraestructura y software contratado de dos (2) años, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la página web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. Tener en cuenta que los acuerdos de niveles de servicios deben ser lo más altos para la fábrica. • Certificación del fabricante sobre los equipos ofertados: o Garantía de los equipos, con Servicio directo de fábrica 7x24 por 24 meses, que incluya Soporte Telefónico y repuestos. o Actualización de firmware y/o software por el término de 24 meses. o Equipos nuevos, no remanufacturados, Administrables, Corporativos, de última generación y tecnología, que cumplen las especificaciones Técnicas mínimas exigidas por la Entidad y que cuentan con los protocolos necesarios para garantizar su funcionamiento, compatibilidad e interoperabilidad con las marcas de switches actuales en la Entidad, protocolos habilitados, licenciados y funcionales al 100%, sin costo adicional para la Entidad. o La instalación configuración y puesta en funcionamiento de los equipos será realizada por ingenieros certificados por el fabricante. o Certificación del fabricante que garantice representación en el país que incluya soporte técnico, existencia de repuestos, partes y accesorios nuevos, no remanufacturados para los equipos objeto del contrato. o El fabricante debe figurar como líder al menos en una (1) de las dos (2) últimas ediciones del cuadrante de Gartner para Enterprise Wired and Wireless LAN. Se debe adjuntar la evidencia con los informes. o Catálogo: Debe anexar el catálogo correspondiente, resaltando e identificando cada una de las especificaciones técnicas aquí solicitadas con el numeral respectivo, a fin de que la Entidad pueda verificar el cumplimiento y calificar en consecuencia.

3.2. REQUISITOS TÉCNICOS DE SWITCH DE ACCESO CON CARACTERISTICAS POE 48 PUERTOS.

ITEM	REQUERIMIENTO TECNICO MINIMO DE OBLIGATORIO CUMPLIMIENTO

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.

1	Suministro de veinte (20) switches de acceso capa 2 POE
2	Arquitectura de gestión centralizada
3	Integración con plataformas de ciberseguridad de la Entidad
4	Capacidades de monitoreo, analítica y optimización operativa
5	Soporte técnico y garantía por 24 meses
6	**Arquitectura y Factor de Forma** • Factor de forma 1RU, montaje en rack estándar de 19” • Fuente de poder redundante • MTBF mínimo esperado: ≥ 10 años • Soporte como mínimo de certificaciones FCC, CE, RCM, VCCI y RoHS2 • Garantía limitada de por vida directo con el fabricante (5 años después del fin de venta)
7	**Interfaces y Conectividad (mínimo requerido)** El switch ofertado deberá contar como mínimo con: • 48 puertos Ethernet RJ45 de acceso cumpliendo con el estándar IEEE 802.3af/at , presupuesto mínimo de PoE de 770W. • 4 puertos de uplink 10 Gigabit Ethernet (SFP+/SFP) o 4 puertos de uplink 10/25 GE (SFP+/SFP28) • Puerto dedicado de gestión • Puerto de consola serial RJ 45 o USB
8	**Capacidades de Conmutación** • Capacidad de switching (full duplex): ≥ 176 Gbps • Reenvío de paquetes (pps): ≥ 262 Mpps • Latencia máxima: ≤ 2 µs • Tabla MAC: mínimo 32.000 direcciones • VLANs soportadas: mínimo 4.000 • Administración ○ Interfaz de línea de Comandos Estándar de la Industria, SNMP V1/2c/3 ○ Administración de VLAN, Soporte a Voice VLAN. ○ Soportar administración basada en SSH y telnet. ○ Soportar OpenFlow o Netconf o Rest APIs. • Soportar SFlow o Netflow. • En caso de no contarse con el controlador SD-LAN, este debe incluirse en la propuesta con todas las funcionalidades y sistema de gestión necesarias

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.

	para este proyecto. Se debe poder administrar Switches, Access Point, SD-WAN y firewalls desde la misma consola de administración.
9	**Funcionalidades de Capa 2** • Soportar RMON (RFC 2819), Sflow (RFC 3176) • IEEE 802.1Q, VLAN IDs >= 4.000. Soportar IEEE 802.1ad QinQ • Private VLAN • Soporte de agregación de enlaces L2 via LACP • Minimo ACLs 1000 • Instancias de spanning tree minimo: 32 • Entrada de Host minimo: 7000 • Debe soportar MLD snooping, MLD proxy, MLD querier o IGMP querier • Debe soportar DHCP Snooping, IPv6 RA guard •Debe contar con IPV6 nativo y homologado por el fabricante (Certificado de fábrica) y se debe soportar la activación del Dual stack. • Debe contar con al menos un medio de monitoreo de conexiones de cobre, y un medio de monitoreo de alerta de fallas en conexiones de fibra. Especificar la nomenclatura del fabricante de estos métodos tanto para conexiones de cobre como para conexiones de fibra. • STP Root Guard, STP, RSTP, MSTP • Debe soportar MCLAG (multichassis link aggregation) • QoS que cumpla con: Clasificación, marcado, policy, strict priority, WRED • Debe soportar QoS marking (IPv4/IPv6) • Debe soportar Egress priority mapping (IPv4/IPv6) • Packet buffer mínimo de 4 MB • Debe soportar notificación de congestión explícita (ECN) para IPv4 e IPv6 • Debe soportar priority-based flow control
10	**Seguridad Integrada en la Red de Acceso** **El switch deberá soportar:** • Control de acceso basado en roles y tipo de dispositivo • Debe estar en 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 • Debe soportar el movimiento de clientes de un puerto a otro sin necesidad de borrar la sesión 802.1X

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 Switch debe permitir descargar políticas de seguridad desde e firewall perimetral de la Entidad • Debe permitir autenticación y autorización Local RADIUS y TACAS+ • Debe soportar Port Mirroring para la supervisión del tráfico de la red • Debe soportar DHCP snooping, Dynamic ARP • Debe soportar IEEE 802.1X (Port Based Network Access Control) • Debe soportar PTP (IPv4 e IPv6) • Funcionalidades Network Access Control (NAC) básicas integradas en la solución (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
11	**Gestión Centralizada de los Switches de acceso** Los Switches de acceso deben ser gestionados desde una plataforma (Controladora SD-LAN) del mismo fabricante de los Switches o sobre plataformas con las que cuente la Entidad en la actualidad y que permitan: • Administración completa desde una única consola en Appliance físico o virtual en las premisas, o una consola en nube. • Definición centralizada de: o VLANs o Políticas de acceso o Segmentación de red o Prioridades de tráfico • Eliminación de la gestión individual por dispositivo • Aplicación automática de políticas de seguridad en la capa de acceso • Soporte de Zero Touch Provisioning y aprovisionamiento remoto seguro • Descubrimiento automático de Switches Los Switches deben integrarse nativamente o via API a los Firewall referencia FG-1101E que posee actualmente la entidad, para gestión centralizado, control unificado de tráfico, control y aplicación de políticas de seguridad y visibilidad. Cuando la integración se realice mediante API el fabricante deberá garantizar, implementar, soportar y mantener la interoperabilidad de la solución propuesta con los Firewall actualmente implementados por la entidad. Para tal efecto el contratista deberá presentar certificación emitida por el fabricante o su representante autorizado en Colombia, firmada por el representante legal, donde conste dicho compromiso. La plataforma de gestión debe tener integración con la plataforma centralizada de registros y reportes FortiAnalyzer 300F y FortiAnalyzer 1000G de la entidad, para

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.

	centralizar los logs de las plataformas de seguridad, red LAN, 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, 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, eventos operativos. 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.
12	**Generalidades de los Switches de Acceso** • Suministrar los cables de potencia, patchcord de FO, patchcord red LAN, conectores, tarjetas, software, licencias, transceivers, y demás elementos físicos, lógicos y técnicos (cables, rieles, tornillería y demás elementos que se requieran) necesarios para su configuración e instalación, 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. • Soporte para apilamiento, apilamiento virtual o gestión de múltiples switches. Deben ser incluidos los cables necesarios (mínimo un cable por Switch) y con una longitud mínima de 3 metros. • La plataforma deber contar con la capacidad de integración nativa con herramientas de Digital Experience Monitoring (DEM) del mismo fabricante, facilitando futuras estrategias de visibilidad y monitoreo de la experiencia del usuario final.

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.

	• Administración de los Switches: o Interfaz de línea de Comandos Estándar de la Industria, SNMP V1/2c/3 o Soportar ACL o Administración de VLAN, Soporte de Voice VLAN o similar o Soportar administración basada en SSH y telnet. o Soportar OpenFlow o Netconf o Rest APIs. o Administración mediante consola para CLI (Command Line Interface). No se admiten equipos de línea Small Business: Equipos cuya administración sea únicamente a través de htttp/https. • Capacidad de escalar como mínimo a 196 de Switches bajo la misma plataforma central de gestión. • Gestión, Monitoreo y Auditoría de los Switches de Acceso y Distribución o Registro de eventos centralizado o Trazabilidad de cambios o Exportación de logs • Se debe garantizar y proveer licenciamiento/servicios necesarios para la integración con plataformas y herramientas con las que cuenta actualmente la Entidad, través de protocolos estándar, conectores o vía API con: o Plataforma de analítica y reportes o Plataformas de seguridad existentes • Suministrar los cables de potencia, patchcord de FO, patchcord red LAN, conectores, tarjetas, software, licencias, transceivers, y demás elementos físicos, lógicos y técnicos (cables, rieles, tornillería y demás elementos que se requieran) necesarios para su configuración e instalación, 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. • Brindar soporte y garantia de dos (2) años para todo el hardware y servicios entregados en funcionamiento, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la página web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. • Brindar licenciamiento de la infraestructura y software contratado de dos (2) años, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la

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.

	página web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. • Brindar garantía de la infraestructura y software contratado de dos (2) años, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la página web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. Tener en cuenta que los acuerdos de niveles de servicios deben ser lo más altos para la fábrica. • Certificación del fabricante sobre los equipos ofertados: o Garantía de los equipos, con Servicio directo de fábrica 7x24 por 24 meses, que incluya Soporte Telefónico y repuestos. o Actualización de firmware y/o software por el término de 24 meses. o Equipos nuevos, no remanufacturados, Administrables, Corporativos, de última generación y tecnología, que cumplen las especificaciones Técnicas mínimas exigidas por la Entidad y que cuentan con los protocolos necesarios para garantizar su funcionamiento, compatibilidad e interoperabilidad con las marcas de switches actuales en la Entidad, protocolos habilitados, licenciados y funcionales al 100%, sin costo adicional para la Entidad. o La instalación configuración y puesta en funcionamiento de los equipos será realizada por ingenieros certificados por el fabricante. o Certificación del fabricante que garantice representación en el país que incluya soporte técnico, existencia de repuestos, partes y accesorios nuevos, no remanufacturados para los equipos objeto del contrato. o El fabricante debe figurar como líder al menos en una (1) de las dos (2) últimas ediciones del cuadrante de Gartner para Enterprise Wired and Wireless LAN. Se debe adjuntar la evidencia con los informes. o Catálogo: Debe anexar el catálogo correspondiente, resaltando e identificando cada una de las especificaciones técnicas aquí solicitadas con el numeral respectivo, a fin de que la Entidad pueda verificar el cumplimiento y calificar en consecuencia.

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.

3.3. REQUISITOS TÉCNICOS DE SWITCH DE ACCESO CON CARACTERISTICAS POE 24 PUERTOS.

ITEM	REQUERIMIENTO TECNICO MINIMO DE OBLIGATORIO CUMPLIMIENTO
1	Suministro de diez (10) switches de acceso capa 2 POE
2	Arquitectura de gestión centralizada
3	Integración con plataformas de ciberseguridad de la Entidad
4	Capacidades de monitoreo, analítica y optimización operativa
5	Soporte técnico y garantía por 24 meses
6	Arquitectura y Factor de Forma • Factor de forma 1RU, montaje en rack estándar de 19” • Fuente de poder redundante • MTBF mínimo esperado: ≥ 10 años • Soporte como mínimo de certificaciones FCC, CE, RCM, VCCI y RoHS2
7	**Interfaces y Conectividad (mínimo requerido)** El switch ofertado deberá contar como mínimo con: • 24 puertos Ethernet RJ45 de acceso cumpliendo con el estándar IEEE 802.3af/at con soporte para PoE+ de 30 W por puerto, presupuesto mínimo de PoE de 421W. • 4 puertos de uplink 10 Gigabit Ethernet (compatibles SFP+/SFP). • Puerto dedicado de gestión • Puerto de consola serial RJ 45 o USB
8	**Capacidades de Conmutación** • Capacidad de switching (full duplex): ≥ 128 Gbps • Reenvío de paquetes (pps): ≥ 190 Mpps • Latencia máxima: ≤ 1 µs • Tabla MAC: mínimo 16.000 direcciones • VLANs soportadas: mínimo 4.000 • Administración mediante consola para CLI (Command Line Interface). No se admiten equipos de línea small business: equipos cuya administración sea únicamente a través de http / https • En caso de no contarse con el Controlador SD-LAN, este debe incluirse en la propuesta con todas las funcionalidades y sistemas de Gestión necesarias para este proyecto. Se debe poder administrar Switches, Access

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.

	Point, SD-WAN y Firewalls desde la misma consola de Administración.
9	**Funcionalidades de Capa 2** • Soportar RMON (RFC 2819), Sflow (RFC 3176) • IEEE 802.1Q. VLAN IDs>= 4.000, Soportar IEEE802.1ad QinQ • Private VLAN • Soporte de agregación de enlaces L2 via LACP • Minimo ACLs 1000 • Instancias de spanning tree minimo 16 • Entrada de Host minimo 2000 • Soportar DHCPv6 snooping, IPv6 RA guard • debe contar con IPV6 nativo y homologado por el fabricante (Certificado de fábrica) y se debe soportar la activación del Dual stack. • Debe contar con al menos un medio de monitoreo o alerta de fallas en conexiones de cobre, y un medio de monitoreo o alerta de fallas en conexiones de fibra. Especificar la nomenclatura del fabricante de estos métodos tanto para conexiones de cobre como para conexiones de fibra. • STP root guard, STP, RSTP, MSTP • Debe soportar MCLAG (multi chassis aggregation) • QoS que cumpla con: Clasificación, marcado, policy, strict priority, WRED • Debe soportar Egress priority Mapping (IPv4/IPv6) • Packet buffer minimo 2 MB • Debe soportar notificación de congestión explícita (ECN) para IPv4 e IPv6
10	**Seguridad Integrada en la Red de Acceso** **El switch deberá soportar:** • Control de acceso basado en roles y tipo de dispositivo • Debe estar en 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 • Debe soportar el movimiento de clientes de un puerto a otro sin necesidad de borrar la sesión 802.1X • El switch debe permitir descargar políticas de seguridad desde el firewall perimetral de 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.

	• Debe permitir la autenticación y autorización Local RADIUS y TACAS+ • Debe soportar DHCP snooping, IP source guard, Dynamic ARP • Debe soportar IEEE 802.1X (Port Based Network Access Control) • Debe soportar PTP (IPv4 e IPv6) • Funcionalidades Network Access Control (NAC) básicas integradas en la solución (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
11	**Gestión Centralizada de los Switches de acceso** Los Switches de acceso deben ser gestionados desde una plataforma (Controladora SD-LAN) del mismo fabricante de los Switches o sobre plataformas con las que cuente la Entidad en la actualidad y que permitan: • Administración completa desde una única consola en Appliance físico o virtual en las premisas, o una consola en nube. • Definición centralizada de: o VLANs o Políticas de acceso o Segmentación de red o Prioridades de tráfico • Eliminación de la gestión individual por dispositivo • Aplicación automática de políticas de seguridad en la capa de acceso • Soporte de Zero Touch Provisioning y aprovisionamiento remoto seguro • Descubrimiento automático de Switches Los Switches deben integrarse nativamente o via API a los Firewall referencia FG-1101E que posee actualmente la entidad, para gestión centralizado, control unificado de tráfico, control y aplicación de políticas de seguridad y visibilidad. Cuando la integración se realice mediante API el fabricante deberá garantizar, implementar, soportar y mantener la interoperabilidad de la solución propuesta con los Firewall actualmente implementados por la entidad. Para tal efecto el contratista deberá presentar certificación emitida por el fabricante o su representante autorizado en Colombia, firmada por el representante legal, donde conste dicho compromiso. La plataforma de gestión debe tener integración con la plataforma centralizada de registros y reportes FortiAnalyzer 300F y FortiAnalyzer 1000G de la entidad, para centralizar los logs de las plataformas de seguridad, red LAN, 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, almacenamiento, análisis y generación de reportes a

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.

	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, eventos operativos. 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.
12	**Generalidades de los Switches de Acceso** • Suministrar los cables de potencia, patchcord de FO, patchcord red LAN, conectores, tarjetas, software, licencias, transceivers, y demás elementos físicos, lógicos y técnicos (cables, rieles, tornillería y demás elementos que se requieran) necesarios para su configuración e instalación, 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. • Soporte para apilamiento, apilamiento virtual o gestión de múltiples switches. Deben ser incluidos los cables necesarios (mínimo un cable por Switch) y con una longitud mínima de 3 metros. • La plataforma deber contar con la capacidad de integración nativa con herramientas de Digital Experience Monitoring (DEM) del mismo fabricante, facilitando futuras estrategias de visibilidad y monitoreo de la experiencia del usuario final. • Administración de los Switches: o Interfaz de línea de Comandos Estándar de la Industria, SNMP V1/2c/3 o Soportar ACL o Administración de VLAN, Soporte de Voice VLAN o similar

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.

	○ Soportar administración basada en SSH y telnet. ○ Soportar OpenFlow o Netconf o Rest APIs. ○ Administración mediante consola para CLI (Command Line Interface). No se admiten equipos de línea Small Business: Equipos cuya administración sea únicamente a través de htttp/https. • Capacidad de escalar como mínimo a 196 de Switches bajo la misma plataforma central de gestión. • Gestión, Monitoreo y Auditoría de los Switches de Acceso y Distribución ○ Registro de eventos centralizado ○ Trazabilidad de cambios ○ Exportación de logs • Se debe garantizar y proveer licenciamiento/servicios necesarios para la integración con plataformas y herramientas con las que cuenta actualmente la Entidad, través de protocolos estándar, conectores o vía API con: ○ Plataforma de analítica y reportes ○ Plataformas de seguridad existentes • • Suministrar los cables de potencia, patchcord de FO, patchcord red LAN, conectores, tarjetas, software, licencias, transceivers, y demás elementos físicos, lógicos y técnicos (cables, rieles, tornillería y demás elementos que se requieran) necesarios para su configuración e instalación, 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. • Brindar soporte y garantia de dos (2) años para todo el hardware y servicios entregados en funcionamiento, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la página web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. • Brindar licenciamiento de la infraestructura y software contratado de dos (2) años, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la página web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. • Brindar garantía de la infraestructura y software contratado de dos (2) años, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la

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.

	página web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. Tener en cuenta que los acuerdos de niveles de servicios deben ser lo más altos para la fábrica. • Certificación del fabricante sobre los equipos ofertados: o Garantía de los equipos, con Servicio de fábrica 7x24 con 24 meses, que incluya Soporte Telefónico y repuestos. o Actualización de firmware y/o software por el término de 24 meses. o Equipos nuevos, no remanufacturados, Administrables, Corporativos, de última generación y tecnología, que cumplen las especificaciones Técnicas mínimas exigidas por la Entidad y que cuentan con los protocolos necesarios para garantizar su funcionamiento, compatibilidad e interoperabilidad con las marcas de switches actuales en la Entidad, protocolos habilitados, licenciados y funcionales al 100%, sin costo adicional para la Entidad. o La instalación configuración y puesta en funcionamiento de los equipos será realizada por ingenieros certificados por el fabricante. o Certificación del fabricante que garantice representación en el país que incluya soporte técnico, existencia de repuestos, partes y accesorios nuevos, no remanufacturados para los equipos objeto del contrato. o El fabricante debe figurar como líder al menos en una (1) de las dos (2) últimas ediciones del cuadrante de Gartner para Enterprise Wired and Wireless LAN. Se debe adjuntar la evidencia con los informes. o Catálogo: Debe anexar el catálogo correspondiente, resaltando e identificando cada una de las especificaciones técnicas aquí solicitadas con el numeral respectivo, a fin de que la Entidad pueda verificar el cumplimiento y calificar en consecuencia.

3.4. REQUISITOS TÉCNICOS DE SWITCH DE DISTRIBUCION

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
1	Suministro de ocho (8) switches de distribución capa2/3
2	Arquitectura de gestión centralizada

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 TÉCNICO MÍNIMO
3	Integración con plataformas de la Entidad
4	Capacidades de monitoreo, analítica y optimización operativa
5	Soporte técnico y garantía por 24 meses.
6	**Arquitectura y Factor de Forma** • Equipo para uso en campus y Datacenter empresarial • Factor de forma 1RU, montaje en rack estándar de 19” • Fuente de poder redundante Hot Swappable • MTBF mínimo esperado: ≥ 10 años • Soporte como mínimo de certificaciones FCC, CE, RCM y RoHS2 • Consumo de potencia de máximo del Switch: 180W • Garantia limitada de por vida directo con el fabricante (5 años después del fin de venta)
7	**Interfaces y Conectividad (mínimo requerido)** **El switch ofertado deberá contar como mínimo con:** • 24 puertos Ethernet 1G/10G SFP/SFP+ • 2 puertos de uplink 40/100 Gigabit Ethernet (compatibles QSFP+/QSFP28) • Puerto dedicado de gestión • Puerto de consola serial RJ 45 o USB
8	**Capacidades de Conmutación y Enrutamiento** • Capacidad de switching mínima (full duplex): ≥ 880 Gbps • Reenvío de paquetes mínimo (pps): ≥ 1300 Mpps • Latencia máxima: ≤ 1 µs • Tabla MAC: mínimo 64.000 direcciones • Entradas de ruta mínimo (IPv4/Ipv6): 8.000/4.000 • VLANs soportadas: mínimo 4.000 • Soporte de Link Aggregation (LACP) • En caso de no contarse con el Controlador SD-LAN, este debe incluirse en la propuesta con todas las funcionalidades y sistemas de Gestión necesarias para este proyecto. Se debe poder administrar Switches, Access Point, SD-WAN y Firewalls desde la misma consola de Administración.
9	**Funcionalidades de Capa 2/3** • Funcionalidades de Calidad de Servicio: o Deberá soportar priorización de tráfico basada en 802.1p

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 TÉCNICO MÍNIMO
	○ Deberá soportar priorización de tráfico basada en IP TOS/DSCP ○ Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP • Los switches deberán soportar las siguientes funcionalidades capa 2: ○ Gestión centralizada desde plataforma de gestión para configuración de VLANs, PoE, Link aggregation, spanning tree, LLDP/MED, IGMP Snooping y actualización de software. ○ Soporte de autenticacion 802.1x. ○ Soporte de DHCP Snooping, detección de dispositivos, listas negras y blancas de direcciones MAC y control de políticas de usuarios y dispositivos. ○ ○ debe contar con IPV6 nativo y homologado por el fabricante (Certificado de fábrica) y se debe soportar la activación del Dual stack. ○ Soporte de Sticky MAC, MAC Limit, inspección ARP dinámica, 802.1p, TOS/DSCP. ○ Deberá soportar Link Aggregation estático y LACP ○ Deberá soportar Spanning Tree ○ Deberá soportar Jumbo Frames ○ Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). ○ Deberá soportar la funcionalidad STP Root Guard, STP BPDU Guard ○ Deberá soportar el estándar IEEE 802.1Q VLAN Tagging ○ Deberá soportar instancias de Spanning Tree (MSTP/CST) ○ Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure ○ Deberá soportar el estándar IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z 1000Base-SX/LX, IEEE 802.3ab 1000Base-T, IEEE 802.3ae 10 Gigabit Ethernet, IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa física ○ Deberá contar con la funcionalidad de Control de Tormentas (Storm Control) ○ Deberá soportar la creación de VLANs por MAC, IP ○ Deberá soportar IGMP Snooping, IGMP proxy y querier ○ Deberá soportar VLAN Stacking (QinQ)

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 TÉCNICO MÍNIMO
	○ Deberá soportar SPAN, RSPAN y ERSPAN • Los switches deberán soportar las siguientes funcionalidades capa 3: ○ Deberá soportar ruteo estático ○ Deberá soportar RIP v2, OSPF, OSPF v3, VRRP, IS-IS, BGP ○ Deberá soportar protocolos de ruteo multicast (IGMPv1/v2/v3, PIM-DM, PIM-SM y MSDP) ○ Deberá soportar Equal Cost Multipath Routing (ECMP) y Bidirectional Forwarding Detection (BFD) ○ Deberá soportar DHCP Relay y DHCP Server • RFCs Soportados: ○ Deberá soportar el RFC 2571 Architecture for Describing SNMP ○ Deberá soportar el RFC 2865 RADIUS ○ Deberá soportar el RFC 1643 Ethernet-like Interface MIB ○ Deberá soportar el RFC 1213 MIB-II ○ Deberá soportar el RFC 1157 SNMPv1/v2c/v3
10	**Seguridad Integrada en Distribución** **El switch deberá soportar:** • Control de acceso basado en roles y tipo de dispositivo • 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 • Funcionalidades Network Access Control (NAC) básicas integradas en la solución (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
11	**Gestión Centralizada de los Switches de Distribución** Los Switches deben ser gestionados por una plataforma (Controladora SD-LAN) que permita administrar los Switches de acceso y distribución, que sea del mismo fabricante de los Switches. La plataforma debe permitir: • Administración completa desde una única consola en Appliance físico o virtual en las premisas, o una consola en nube. • Definición centralizada de: ○ VLANs

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 TÉCNICO MÍNIMO
	○ Políticas de acceso ○ Segmentación de red ○ Prioridades de tráfico • Eliminación de la gestión individual por dispositivo • Aplicación automática de políticas de seguridad en la capa de acceso • Soporte de Zero Touch Provisioning y aprovisionamiento remoto seguro • Descubrimiento automático de Switches Los Switches deben integrarse nativamente o via API a los Firewall referencia FG-1101E que posee actualmente la entidad, para gestión centralizado, control unificado de tráfico, control y aplicación de políticas de seguridad y visibilidad. Cuando la integración se realice mediante API el fabricante deberá garantizar, implementar, soportar y mantener la interoperabilidad de la solución propuesta con los Firewall actualmente implementados por la entidad. Para tal efecto el contratista deberá presentar certificación emitida por el fabricante o su representante autorizado en Colombia, firmada por el representante legal, donde conste dicho compromiso. La plataforma de gestión debe tener integración con la plataforma centralizada de registros y reportes FortiAnalyzer 300F y FortiAnalyzer 1000G de la entidad, para centralizar los logs de las plataformas de seguridad, red LAN, 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, 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, eventos operativos. 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

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 TÉCNICO MÍNIMO
	de malware avanzado y mejorar la visibilidad y respuesta frente a incidentes de seguridad en entornos distribuidos. La plataforma de gestión deberá ser capaz de integrar motores de Inteligencia Artificial para el análisis de causa raíz, detección proactiva de anomalías y recomendaciones de remediación.
12	**Generalidades de los Switches de Distribución** • Suministrar los cables de potencia, patchcord de FO, patchcord red LAN, conectores, tarjetas, software, licencias, transceivers, y demás elementos físicos, lógicos y técnicos (cables, rieles, tornillería y demás elementos que se requieran) necesarios para su configuración e instalación, 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. • Soporte para apilamiento, apilamiento virtual o gestión de múltiples switches. Deben ser incluidos los cables necesarios (mínimo un cable por Switch) y con una longitud mínima de 3 metros. • La plataforma deber contar con la capacidad de integración nativa con herramientas de Digital Experience Monitoring (DEM) del mismo fabricante, facilitando futuras estrategias de visibilidad y monitoreo de la experiencia del usuario final • Administración de los Switches: ○ Interfaz de línea de Comandos Estándar de la Industria, SNMP V1/2c o 3 ○ Soportar ACL ○ Administración de VLAN, Soporte de Voice VLAN o similar ○ Soportar administración basada en SSH y telnet. ○ Soportar OpenFlow o Netconf o Rest APIs. ○ Administración mediante consola para CLI (Command Line Interface). No se admiten equipos de línea Small Business: Equipos cuya administración sea únicamente a través de htttp/https. • Capacidad de escalar como mínimo a 196 de Switches bajo la misma plataforma central de gestión. • Gestión, Monitoreo y Auditoría de los Switches de Acceso y Distribución ○ Registro de eventos centralizado ○ Trazabilidad de cambios ○ Exportación de logs

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 TÉCNICO MÍNIMO
	• Se debe garantizar y proveer licenciamiento/servicios necesarios para la integración con plataformas y herramientas con las que cuenta actualmente la Entidad, través de protocolos estándar, conectores o vía API con: o Plataformas de monitoreo o Plataforma de analítica y reportes o Plataformas de seguridad existentes •Brindar soporte y garantía de veinticuatro (24) meses para todo el hardware y servicios entregados en funcionamiento, tiempo que será contado a partir de la entrega de la solución y puesta en marcha a satisfacción, acta de funcionamiento aprobada por el supervisor y el registro en la página web del fabricante, actividad que se realiza sin costo adicional para la Secretaría Distrital de Salud. • Certificación del fabricante sobre los equipos ofertados: o Garantía de los equipos, con Servicio directo de fábrica 7x24 con veinticuatro (24) meses, que incluya Soporte Telefónico y repuestos. o Actualización de firmware y/o software por el término de veinticuatro (24) meses. o Equipos nuevos, no remanufacturados, Administrables, Corporativos, de última generación y tecnología, que cumplen las Especificaciones Técnicas mínimas exigidas por la Entidad y que cuentan con los protocolos necesarios para garantizar su funcionamiento, compatibilidad e interoperabilidad con las marcas de switches actuales en la Entidad, protocolos habilitados, licenciados y funcionales al 100%, sin costo adicional para la Entidad. o La instalación configuración y puesta en funcionamiento de los equipos será realizada por ingenieros certificados por el fabricante. o Certificación del fabricante que garantice representación en el país que incluya soporte técnico, existencia de repuestos, partes y accesorios nuevos, no remanufacturados para los equipos objeto del contrato. o El fabricante debe figurar como líder al menos en una (1) de las dos (2) últimas ediciones del cuadrante de Gartner para Enterprise Wired and Wireless LAN. Se debe adjuntar la evidencia con los informes. o Catálogo: Debe anexar el catálogo correspondiente, resaltando e identificando cada una de las especificaciones técnicas aquí solicitadas con el numeral respectivo, a fin de que la Entidad pueda verificar el cumplimiento y calificar en consecuencia.

3.5. REQUISITOS TÉCNICOS TRANSCEIVERS

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
1	Suministro de cuarenta y ocho (48) SFP+/SFP28
2	Arquitectura y Factor de Forma• Veinticuatro (24) Transceivers 25 Gigas SFP28 25G-SR-C totalmente compatibles con los switches core QFX5120-48YM-AFO instados en la SDS. • Veinticuatro (24) Transceivers 10 Gigas SFP+ 10G-SR-C totalmente compatibles con los switches core QFX5120-48YM-AFO instados en la SDS.

3.6 REQUISITOS TÉCNICOS DE INTEGRACION

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 Switching 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. 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 Switches 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 Switching 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

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.

	contratista deberá presentar certificación emitida por el fabricante o su representante autorizado en Colombia, firmada por el representante legal, donde conste dicho compromiso.

4. CARACTERÍSTICAS GENERALES

El contratista debe cumplir los siguientes requisitos:

a) Se debe realizar la puesta en funcionamiento del licenciamiento y dispositivos adquiridos, así como la integración con las plataformas de seguridad y monitoreo con las que cuenta la Secretaría Distrital de Salud.
b) El licenciamiento requerido debe tener soporte en un esquema 7 x 24 ante fabricante que incluya actualizaciones de firmware y reemplazo de partes (cuando es Hardware).

5. REQUERIMIENTOS TÉCNICOS DE INSTALACIÓN

- El contratista debe realizar la instalación física de todos los Switches y elementos necesarios en los centros de datos de la SDS. Cumpliendo con las generalidades de los numerales 3,1,3,2,3,3 y 3,4 del presente anexo técnico; donde se garantice la integración y funcionamiento con los equipos activos existentes en la SDS.
- El contratista debe realizar la configuración y alistamiento del software, firmware del hardware a la última versión estable aprobada por el fabricante para todas las plataformas licenciadas.
- El contratista deberá realizar la configuración y activación de las licencias en cada una de las plataformas, así como el respectivo registro en la página web del fabricante.

6. TRANSFERENCIA DE CONOCIMIENTO

El contratista deberá realizar transferencia de conocimiento durante mínimo ocho (8) horas por solución, a tres (3) ingenieros del Grupo de TIC, designados por el Supervisor del contrato, orientada a la instalación, configuración, parametrización y puesta en marcha de la solución, que brinde el conocimiento necesario para la administración y operación del hardware y software de la solución de seguridad implementada.

La transferencia de conocimiento se podrá realizar durante la instalación, configuración, parametrización y puesta en funcionamiento la solución.

Previo al inicio de actividades, el contratista deberá hacer entrega del documento de Plan de Transferencia de conocimiento en el cual se debe describir el mecanismo a utilizar para dicha actividad, de tal manera que se logre efectuar un aprovechamiento óptimo del software, de los equipos y de la tecnología.

7. SERVICIOS PROFESIONALES

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 deberá contemplar dentro de su oferta, como mínimo, los siguientes servicios profesionales asociados a la implementación de la solución:

1. Diseño, instalación y puesta en funcionamiento. Servicios de diseño, instalación, configuración, parametrización, puesta en funcionamiento e integración de la solución, con entrega a satisfacción de la entidad. Estas actividades deberán ser ejecutadas por ingenieros certificados por el fabricante de los equipos, para lo cual el contratista deberá presentar las certificaciones vigentes del equipo de trabajo asignado, expedidas directamente por el fabricante.
2. Diseño de seguridad perimetral. Diseño de la arquitectura de seguridad perimetral conforme a las buenas prácticas y recomendaciones del fabricante, garantizando la integración con los dispositivos de seguridad con los que actualmente cuenta la entidad. Este diseño deberá ser sometido a evaluación y aprobación del supervisor del contrato.
3. Diseño de políticas de seguridad. Elaboración y presentación del diseño de políticas de seguridad, el cual será evaluado y aprobado por el líder de infraestructura y el supervisor del contrato.
4. Alistamiento de software, hardware y firmware. Configuración y alistamiento de las plataformas en la última versión estable aprobada por el fabricante, para cada uno de los componentes de software, hardware y firmware involucrados.
5. Implementación conforme a buenas prácticas. Implementación de la solución siguiendo las mejores prácticas del fabricante, garantizando una arquitectura de red segura.
6. Pruebas de servicio. Ejecución de pruebas de servicio sobre las plataformas ofertadas, con el fin de validar su correcto funcionamiento previo a la puesta en producción.
7. Puesta en producción. Despliegue en ambiente de producción de las plataformas ofertadas.
8. Estabilización. Acompañamiento y ajustes necesarios para la estabilización de las plataformas ofertadas una vez puestas en producción.
9. Integración con la infraestructura existente. Diseño, instalación, configuración, integración y puesta en producción de los dispositivos de seguridad y red con los que actualmente cuenta la entidad, incluyendo la entrega a satisfacción y la ejecución de todas las tareas necesarias para tal fin, sin que ello genere costos o cobros adicionales para la entidad.
10. Configuración operativa integral y validación. Implementación y puesta en marcha de las plataformas ofertadas, incluyendo la configuración de políticas, objetos y demás parámetros necesarios para dejarlas totalmente operativas y a satisfacción de la entidad. Adicionalmente, el contratista deberá ejecutar pruebas de detección sobre cada plataforma, con el fin de validar su correcta configuración conforme a las buenas prácticas de implementación del fabricante.
11. Logística asociada al servicio. El contratista deberá incluir en su oferta todos los costos y gastos asociados a la logística requerida para el cumplimiento de las labores del personal

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.

asignado al proyecto (desplazamientos, transporte, parqueaderos, equipos y herramientas de trabajo, entre otros).

8. DOCUMENTACIÓN

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

2. El contratista debe documentar todos los procedimientos realizados para la instalación, configuración y parametrización de cada una de las funcionalidades implementadas y entregarlos en medio magnético e impreso, una vez revisados y aprobados por el Supervisor del contrato.

3. Al finalizar la puesta en funcionamiento de la solución contratada, debe entregar en medio magnético o impreso, la documentación que permita la eficiente administración, como mínimo incluir: * Manual de procedimientos de administración y operación de los appliances. Documento de descripción de la configuración de appliance y parámetros de configuración inicial de todo el software instalado. * Documentación de la topología de la solución implementada.

9. REQUERIMIENTOS TÉCNICOS EN FUNCIONAMIENTO

El contratista deberá contemplar, entre otras, la realización y documentación de las siguientes actividades, previa coordinación con el supervisor del contrato:

1. Revisar y configurar las licencias incluidas con los switches adquiridos.
2. Configurar, afinar y revisar los reportes / logs de las plataformas.
3. Implementar la solución de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura.
4. Poner en producción las plataformas, realizando la integración con las demás plataformas de seguridad de la Secretaría Distrital de Salud.
5. Poner en producción las licencias incluidas con los switches adquiridos, realizando la integración con las demás plataformas de seguridad de la Secretaría Distrital de Salud.
6. Mantener actualizado el firmware de los componentes ofertados, de acuerdo con las últimas versiones estables liberadas por el fabricante con aprobación de la Secretaría Distrital de Salud.
7. Posterior a la instalación y puesta en marcha, realizar el afinamiento y estabilización de los equipos adquiridos.
8. Entregar los equipos adquiridos a satisfacción de la Secretaría Distrital de Salud.

NOTA: Las licencias deberán ser a perpetuidad, es decir, no estarán sujetas a vencimiento ni requerirán renovación para mantener las funcionalidades licenciadas durante la vida útil de los equipos.

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.

10. INDICADORES Y ANS MESA DE AYUDA

Los Acuerdos de Nivel de Servicio (ANS) que se establecen en el presente documento hacen parte integral del soporte y garantía de los equipos objeto del contrato, la cual tendrá una vigencia de veinticuatro (24) meses. En este sentido, el contratista deberá garantizar, durante todo el periodo de soporte y garantía, el cumplimiento de los tiempos de respuesta y solución definidos según la clasificación de los incidentes y solicitudes reportados, conforme a las condiciones generales que se detallan a continuación.

El cumplimiento de estos indicadores se regirá por los principios de transparencia, eficiencia y buena fe que rigen el marco normativo de la contratación estatal. En caso de vacíos o situaciones no contempladas en el presente documento, se aplicarán las normas ITIL como estándar de buenas prácticas para la gestión de servicios tecnológicos.

CONDICIONES DEL SERVICIO

El contratista deberá disponer de canales de comunicación para brindar asesoría técnica en instalación, configuración, operación, y diagnóstico de los equipos de la solución de seguridad perimetral, así como escalamiento directo a fábrica sin costo adicional para la entidad.

El tiempo de solución se contabilizará según el nivel de atención y se suspenderá durante actividades cuya responsabilidad corresponda a la Secretaría Distrital de Salud.

Información requerida al reportar una falla:

1. Tipo de problema (aleatorio, frecuente, falla total o parcial)
2. Descripción, frecuencia y ubicación física del problema
3. Información técnica (diagramas de red LAN, WAN o de servicios)
4. Descarte de fallas externas
5. Estado del sistema (errores, debugs, logs de eventos)

Atención telefónica y por correo: El contratista deberá disponer de línea telefónica y correo electrónico con atención 5x8 durante el periodo de garantía, para consultas técnicas, reporte de fallas y seguimiento.

Diagnóstico y cierre de casos: El contratista realizará diagnóstico remoto, validará la viabilidad de solución remota e indicará las acciones requeridas al personal designado. La solución se corroborará mediante chequeo de funcionamiento y el cierre del caso quedará sujeto a la autorización de la entidad.

Certificaciones requeridas: El contratista deberá contar con las certificaciones de Parnert Preferente de Servicios Profesionales Autorizados (o equivalente) y Parnert de Centro de Soporte Autorizado (o equivalente), otorgadas por el fabricante, que garanticen respaldo directo

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.

para la prestación de servicios profesionales, soporte técnico especializado e implementación de las soluciones.

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 el personal de la Secretaría Distrital de Salud que se designe será autorizado por el contratista para tener acceso y control sobre sus tickets abiertos y cerrados, permitiéndoles realizar consultas que puedan servir de ayuda para la solución de un caso actual.

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 Términos de invitación.

La supervisión designará el personal que estará autorizado para gestionar asuntos relacionados con el presente contrato y recibir los informes que se generen del mismo, indicando los datos de contacto a los que se reportarán los soportes establecidos por los mecanismos descritos, su avance y su cierre.

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 5x8 de consultas técnicas, reportes de fallas y seguimiento de estas.

El Soporte Técnico Telefónico no tiene un límite de llamadas.

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 de 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.

Soporte técnico en sitio

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 deberá ofrecer el servicio de soporte técnico en sitio con el personal idóneo para realizar la instalación, operación y resolución de fallas.

Este soporte se activa por el servicio de soporte remoto o por la falta de este, en caso de que sea imposible realizarlo. En este, se dará el diagnóstico de la probable causa del incidente y el plan (repuestos) al área encargada por el contratista.

Durante el ciclo de vida de la incidencia se cumplen completamente con los Acuerdos de Niveles de Servicio SLA acordados y descritos en el siguiente capítulo.

11. ACUERDO DE NIVELES DE SERVICIO MINIMO DEL SOPORTE Y GARANTIA:

El tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio y plan de comunicaciones se describen a continuación.

Tabla 2 Nivel de severidad

TIPO DE FALLA	NIVEL DE SEVERIDAD	DESCRIPCIÓN
FALLA CRITICA	S1	Los equipos dejaron de funcionar por completo, ocasionando un impacto critico en las operaciones de la solución de seguridad de la Secretaría Distrital de Salud.
FALLA GRAVE	S2	Los equipos han dejado de funcionar parcialmente, ocasionando un impacto medio en las operaciones de la solución de seguridad de la Secretaría Distrital de Salud. Algunas operaciones continúan funcionando normalmente.
FALLA LEVE	S3	El sistema no funciona de manera óptima, aunque muchas de las operaciones continúan funcionando correctamente, el impacto es bajo en la solución de seguridad de la Secretaría Distrital de Salud
REQUERIMIENTOS DE SERVICIO	S4	El usuario final requiere información o asistencia sobre las posibilidades, la instalación o configuración de nuevos requerimientos. Se tratan también los problemas comunes con muy bajo

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.

		impacto en la solución de seguridad de la Secretaría Distrital de Salud

Tiempos de respuesta

El registro de cualquier incidencia se puede realizar en cualquier momento del día a cualquier hora por los medios dispuestos para ello por el contratista, sin embargo, solo se tendrá en cuenta en el horario de atención establecido en el contrato.
Los tiempos de respuesta de acuerdo con la clasificación del incidente registrado son los siguientes:

Tabla 3 Tiempos de respuesta

TIEMPO DE RESPUESTA		
NIVEL DE SEVERIDAD	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
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

12. EQUIPO DE TRABAJO

GERENTE DE PROYECTO

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.

Gerente de proyecto dedicación 100%, Profesionales Ingeniero de Sistemas, Electrónico o de Telecomunicaciones, con tarjeta vigente.

Pregrado: Ingeniero electrónico, de sistemas, de telecomunicaciones o afines.
Posgrado: Máster y/o especialización en gerencia de proyectos de tecnologías de la información
EXPERIENCIA: Mínimo diez (10) años de experiencia general a partir de la T.P. y (5) años de experiencia especifica en proyectos de tecnología como Gerente o Director de Proyectos, esta será acredita mediante certificaciones de experiencia laboral.
CERTIFICACIONES REQUERIDAS: El profesional postulado debe contar con tres (3) de las certificaciones que se relacionan a continuación:
ITIL FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT
CISM CERTIFIED INFORMATION SECURITY MANAGER
CNDA - CERTIFIED NETWORK DEFENSE ARCHITECT
PMP –PROJECT MANAGEMENT PROFESSIONAL

PROFESIONAL DE IMPLEMENTACION

Ingeniero electrónico, sistemas o telecomunicaciones o afines
Máster y/o especialización en seguridad informática o ciberseguridad e informática o afines
Mínimo cinco (5) años de experiencia general a partir de la T.P. y (3) años de experiencia especifica en proyectos de seguridad informática, esta será acredita mediante certificaciones de experiencia laboral.
CERTIFICACIONES REQUERIDAS: a nivel profesional y especialista en las soluciones de networking ofertadas Certificación en redes LAN en la marca implementada.

INGENIERO DE SOPORTE

Ingeniero electrónico, sistemas o telecomunicaciones o afines
Máster y/o especialización en seguridad informática o seguridad de la información o afines
Mínimo cinco (5) años de experiencia general a partir de la T.P. y (3) años de experiencia especifica en proyectos de seguridad informática, esta será acredita mediante certificaciones de experiencia laboral.
CERTIFICACIONES REQUERIDAS: a nivel profesional en las soluciones de networking ofertadas

ESPECIALISTA DE TELECOMUNICACIONES

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.

Ingeniero electrónico, sistemas o telecomunicaciones o afines
Máster y/o especialización en seguridad informática o seguridad de la información o afines
Mínimo nueve (9) años de experiencia general todas contadas a partir de la expedición de la T.P., y mínimo tres (3) años de experiencia especifica en proyectos de seguridad informática, mediante la presentación de certificaciones laborales y/o contratos.
CERTIFICACIONES REQUERIDAS: El profesional postulado debe contar con dos (2) de las certificaciones que se relacionan a continuación:
ISO27001:2022 (AUDITOR LIDER)
CEH (CERTIFIED ETHICAL HACKER)
ISO27032:2023 (CYBERSECURITY MANAGER)
ITIL Foundation Certificate in IT Service Management

Nota: Las hojas de vida del personal de trabajo no son requisito habilitante y deben ser entregadas por el contratista dentro de los tres (3) días calendario siguientes a la suscripción del acta de inicio del contrato.

Elaborado por: Arnol Julian Martinez- Contratista TIC
Elaborado por: Jose Fredy, Gonzalez Ruiz - Contratista TIC

Firmado digitalmente por Arnol Julian Martinez Paredes

JOSE FREDY GONZALEZ RUZ

Firmado digitalmente por JOSE FREDY GONZALEZ RUZ

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.