1. CARACTERÍSTICAS Y/O ESPECIFICACIONES TÉCNICAS DE LOS BIENES A CONTRATAR

A continuación, se relacionan las especificaciones técnicas de la solución integral de infraestructura LAN/SD-LAN que se van a adquirir por parte de la entidad, para suplir la necesidad de mejorar la velocidad de conectividad: solución integral de infraestructura LAN/SD-LAN

- Los switches deben soportar la configuración en un entorno de SD-LAN (IBN/SDN) utilizando políticas de grupo. el diseño de la solución es discrecional del CONTRATISTA (como por ejemplo Topologías Leaf-Spine), siempre y cuando cumpla con los requisitos funcionales, de seguridad y técnicos establecidos para el servicio
- Los switches deben incluir una plataforma de gestión única que tenga la capacidad de ver el estado de cada uno de los elementos de red a nivel LAN y WLAN a futuro, de manera que se genere unicidad y facilidad en la configuración de estos

solución	**Switch Core DC y Campus (Cantidad: 2)**
Generalidades	Los equipos no deben ser refurbished, deben ser nuevos y haber sido lanzados en los últimos dos años al mercado. La solución ofertada debe implementarse en dual stack (IPV4 – IPV6).
	Por equipo el Switch de Core fibra debe incluir mínimo: • 24 puertos SFP/SFP+ 1G/10G • 2 puertos QSFP28/QSFP+ 100G/40G • Un puerto de administración fuera de Banda 10/100/1000BASE-T • Un puerto Serial RJ45 El oferente debe suministrar para los Switch de Fibra como minimo: • 38 módulos (Transceivers) 10G SFP+ Duplex LC Connector • 8 módulos (Transceivers) 1G SFP Duplex LC Connector • 2 cable DAC de 10G DAC SFP+ de 3 a 5 metros • 1 cable DAC de 100G DAC QSFP28 de 3 a 5 metros • 2 cable DAC breakout de 100G QSFP28 a 25Gx4 SPF28 de 3 a 5 metros No se aceptan transceivers homologados ni de terceros, deben ser de la misma marca de los Switch ofertados.
	Debe ser máximo de 1 Unidad de rack EIA estándar de 19 in.

	Capacidad de Conmutación >= 850 Gbps
	Capacidad de transmisión de Paquetes Throughput >=1300 Mpps
	latencia <= 1 Microseg
	Consumo de potencia máximo 180W
	Fuente de poder redundante
	Garantía limitada de por vida (5 Años después de fin de venta)
	Jumbo Frames
	MAC address table size >= 64.000
	La solución Switches de Core, Distribución, Acceso y/o Campus debe incluir la administración, configuración y monitoreo unificada de firewall, switching y AP desde una controladora o consola de administración propia de la solución ofertada tanto software como hardware, con el fin de poder brindar un alto nivel de seguridad
	La solución switches de Core, Distribución, Acceso y/o Campus deben tener la capacidad de integrarse nativamente a la solución de Seguridad Perimetral de la entidad y garantizar capacidades avanzadas de seguridad y administración centralizada
Funciones L2	Soportar RMON (RFC 2819), Sflow (RFC 3176).
	IEEE 802.1Q, VLAN Ids>= 4.000 Soportar IEEE 802.1ad QinQ, 802.1AX Link aggregation
	Private Vlan
	Soporte de agregación de enlaces L2 vía LACP mínimo 8 Al menos agregación de 16 enlaces por troncal.
	Minimo ACLs 3000
	Instancias de Spanning Tree minimo 32
	Entrada de Host minimo 24000
	Soportar Cables virtuales (virtual Wire) entre puertos.
	Debe soportar MLD snooping, MLD proxy, MLD querier
	Debe soportar DHCPv6 Snooping, IPV6 RA guard,
	Debe soportar captura de paquetes
	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 (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree)
	Debe soportar e incluir priority-based flow control 802.1Qbb
	Debe soportar MCLAG (multichassis link aggregation)
	Debe soportar Port Mirroring para la supervisión del tráfico de la red
Calidad del Servicio	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 minimo de 8MB

	Debe soportar Notificación de Congestión explicita (ECN) para IPv4 e IPv6
Gestión	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
	Administración: Interfaz de línea de Comandos Estándar de la Industria, SNMP V1/2c/3 Soportar ACL IPV4/IPV6 Administración de VLAN, Soporte a Voice VLAN. Soportar administración basada en SSH y telnet. Soportar OpenFlow o Netconf o Rest Apis. Soportar SFlow y Netflow.
	Debe soportar Administración desde Sistemas de Gestión en Nube o on-Premise
Funciones L3	Debe soportar RIP (IPV4/IPV6), VRRP (IPV4/IPV6) y OSPF (IPV4/IPV6). Debe soportar enrutamiento estático y dinámico
	Soportar BGP (IPv4/IPv6)
	Soportar ISIS (IPv4/IPv6)
	Soportar BFD (IPv4/IPV6)
	Soportar OSPF (IPv4/IPv6)
	Soportar PIM-SSM
	Soportar VRRP (IPv4/IPv6)
	Soportar ECMP con base en Hardware (IPv4/IPv6)
	Debe soportar Interfaces Enrutadas (RVI)
	Soporte de VRF (IPv4/IPv6)
	Soportar BFD para RipNG (IPV6), BGPv6
	Soporte de uRPF
	Rutas IPV4 soportadas estáticas y dinámicas >= 24000
	Debe soportar DHCP-Server
	Rutas IPV6 soportadas >= 8000
Seguridad	Debe estar en capacidad de detectar Dispositivos IoT
	Debe soportar el movimiento de clientes de un puerto a otro sin necesidad de borrar la sesion 802.1X.
	El equipo deberá soportar características de seguridad mínimas: • La solucion debe poder desplegar controles de seguridad para el tráfico Este-Oeste y Norte-Sur al interior del DC, para poder detectar intentos de intrusión, malware entre otros comportamientos anómalos. • Bloque de Tráfico Intra-vlan
	Debe permitir la autenticación y autorización Local RADIUS y TACACS+
	Debe soportar Port Mirroring para la supervisión del tráfico de la red
	Debe soportar SSH

	Debe soportar DHCP snooping, DHCPv6, IP source guard, Dynamic ARP
	Soportar la configuracion de interfaces fisica para enrutamiento
	Debe soportar IEEE 802.1X (Port Based Network Access Control)
	Debe soportar PTP (IPV4 e IPv6)
	Debe soportar FIPS-140-2 (Nivel 2)
	Debe soportar una funcionalidad de ahorro de Energía que baje consumo si no hay tráfico y si llega tráfico hacia el PC se envie mensaje de encendido (Wake-On-Lan - WOL)
Garantías	MTBF minimo de 10 Años (87600 horas)
	El equipo debe contar con Garantía Limitada de por Vida de minimo 5 Años después de fin de venta.
	Cumplimiento de normas FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2
	Todas las funcionalidades que soporte el equipo deben estar incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripcion.
	El soporte local y/o remoto será prestado por el proveedor durante un periodo de 36 meses

solución	**Switch Acceso DC y Campus (Cantidad: 5)**
Caracteristicas	Los equipos no deben ser refurbished, deben ser nuevos y haber sido lanzados en los últimos dos años al mercado.
	Por equipo el Switch de Core fibra debe incluir mínimo: • 48 puertos RJ-45 1G • 4 puertos SFP+ 10G • Un puerto Serial RJ45 Consola
	El oferente debe suministrar para los Switch de Fibra como minimo: • 10 módulos (Transceivers) 10G SFP+ Duplex LC Connector
	No se aceptan transceivers homologados ni de terceros, deben ser de la misma marca de los Switch ofertados
	Cada Switch debe incluir puerto serial para administración: de consola RJ-45.
	Debe ser máximo de 1 Unidad de rack EIA estándar de 19 in.
	Capacidad de Conmutación >= 170 Gbps
	Capacidad de transmisión de Paquetes Throughput >=260 Mpps
	latencia <= 1 Microseg
	Packet buffer minimo de 2MB
	QoS que cumpla con: clasificación, marcado, policy, strict priority, WRED
	Consumo de potencia máximo 57W
	Garantía limitada de por vida (5 años después de fin de venta)
	Soportar RMON (RFC 2819), Sflow (RFC 3176).
	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

	Jumbo Frame - Ethernet / >=10KB
	MAC address table size >= 32.000
	Soporte de agregación de enlaces L2 vía LACP mínimo 16 grupos Al menos agregación de 8 enlaces por troncal.
	Minimo ACLs 760
	Instancias de spanning tree minimo 16
	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 (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree)
Seguridad	La solución Switches de Core, Distribución, Acceso y/o Campus debe incluir la administración, configuración y monitoreo unificada de firewall, switching y AP desde una controladora o consola de administración propia de la solución ofertada tanto software como hardware, con el fin de poder brindar un alto nivel de seguridad
	La solución switches de Core, Distribución, Acceso y/o Campus deben tener la capacidad de integrarse nativamente a la solución de Seguridad Perimetral de la entidad y garantizar capacidades avanzadas de seguridad y administración centralizada
	El equipo deberá soportar características de seguridad mínimas: • La solución debe poder desplegar controles de seguridad para el tráfico Este-Oeste y Norte-Sur al interior del DC, para poder detectar intentos de intrusión, malware entre otros comportamientos anómalos. • Bloque de Tráfico Intra-vlan
	Debe estar en capacidad de detectar Dispositivos IoT
	Debe soportar Administración desde Sistemas de Gestión en Nube y On-Prem
	Administración: Interfaz de línea de Comandos Estándar de la Industria, SNMP V1/2c/3 Soportar ACL IPV4/IPV6 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 permitir la autenticación y autorización Local RADIUS y TACACS+
	Debe soportar SSH
	Debe soportar DHCP snooping, Dynamic ARP
	Debe soportar una funcionalidad de ahorro de Energía que baje consumo si no hay tráfico y si llega tráfico hacia el PC se envie mensaje de encendido (Wake-On-Lan - WOL)
	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.

	Debe soportar IEEE 802.1X (Port Based Network Access Control)
Garantías	MTBF minimo de 10 Años (87600 horas)
	Todas las funcionalidades que soporte el equipo deben estar incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripcion.
	Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2
	El equipo debe contar con Garantía Limitada de por Vida de minimo Años después de fin de venta.
	El soporte local y/o remoto será prestado por el proveedor durante un periodo de 36 meses

solución	**Switch Acceso DC y Campus PoE (Cantidad: 1)**
Caracteristicas	Los equipos no deben ser refurbished, deben ser nuevos y haber sido lanzados en los últimos dos años al mercado. Integración en descubrimiento automático y en seguridad de extremo a extremo mediante el protoclo NAC con el Firewall Fortigate
	Por equipo el Switch de Core fibra debe incluir mínimo: • 24 puertos 2.5G/1G/100M/10M puertos RJ-45 • 6 puertos 10G/1G SFP+/SFP • Un puerto Serial RJ45 Consola
	PoE+ (803.at/af): Configurable en cualquier puerto hasta la potencia máxima. PoE+ (803.bt): Configurable en cualquier puerto hasta la potencia máxima
	Debe ser máximo de 1 Unidad de rack EIA estándar de 19 in.
	Capacidad de Conmutación >= 240 Gbps
	Capacidad de transmisión de Paquetes Throughput >=350 Mpps
	Latencia <= 1 Microseg
	Packet buffer minimo de 2MB
	QoS que cumpla con: clasificación, marcado, policy, strict priority, WRED
	Consumo de potencia máximo 880 W
	Garantía limitada de por vida (5 años después de fin de venta)
	Presupuesto de potencia PoE+ ofertado no deberá ser menor a 780W.
	Soportar RMON (RFC 2819), Sflow (RFC 3176).
	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
	Jumbo Frame - Ethernet / >=10KB
	MAC address table size >= 32.000
Funcion L2	Soporte de agregación de enlaces L2 vía LACP mínimo 16 grupos Al menos agregación de 8 enlaces por troncal.
	Minimo ACLs 760
	Instancias de Spanning Tree minimo 16

Comentado [OC1]: Se sugiere agregar la siguiente característica: Integración en descubrimiento automático y en seguridad de extremo a extremo mediante el protoclo NAC con el Firewall Fortigate

	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 (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree)
Seguridad	La solución Switches de Core, Distribución, Acceso y/o Campus debe incluir la administración, configuración y monitoreo unificada de firewall, switching y AP desde una controladora o consola de administración propia de la solución ofertada tanto software como hardware, con el fin de poder brindar un alto nivel de seguridad
	La solución switches de Core, Distribución, Acceso y/o Campus deben tener la capacidad de integrarse nativamente a la solucion de Seguridad Perimetral de la entidad y garantizar capacidades avanzadas de seguridad y administración centralizada
	Debe estar en capacidad de detectar Dispositivos IoT
	Debe soportar Administración desde Sistemas de Gestión en Nube y On-Premise
	Administración: Interfaz de línea de Comandos Estándar de la Industria, SNMP V1/2c/3 Soportar ACL IPV4/IPV6 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 permitir la autenticación y autorización Local RADIUS y TACACS+
	Debe soportar SSH
	Debe soportar DHCP snooping, Dynamic ARP
	Debe soportar una funcionalidad de ahorro de Energía que baje consumo si no hay tráfico y si llega tráfico hacia el PC se envie mensaje de encendido (Wake-On-Lan - WOL)
	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.
	Debe soportar IEEE 802.1X (Port Based Network Access Control)
Garantías	MTBF minimo de 10 Años (87600 horas)
	Todas las funcionalidades que soporte el equipo deben estar incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripcion.
	Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2
	El equipo debe contar con Garantía Limitada de por Vida de minimo 5 Años después de fin de venta.
	El soporte local y/o remoto será prestado por el proveedor durante un periodo de 36 meses

solución	Punto de acceso inalámbrico (Cantidad: 6)
Generalidades	Los equipos no deben ser refurbished, deben ser nuevos y haber sido lanzados en los últimos dos años al mercado.
	Punto de acceso inalámbrico empresarial para interiores
	Wi-Fi 6E, Wi-Fi 7 o tecnología equivalente o superior, según disponibilidad y compatibilidad técnica
	Soporte para bandas de 2.4 GHz, 5 GHz y 6 GHz, cuando aplique según regulación y diseño
	Antenas internas o diseño equivalente apto para instalación en techo o pared
	Puerto Ethernet de 1 GbE, 2.5 GbE o superior
	Alimentación mediante PoE/PoE+ o adaptador compatible
	Debe mantener compatibilidad con clientes 802.11a/b/g/n/ac/ax, o equivalentes vigentes, sin afectar la operación de clientes compatibles con estándares anteriores, de acuerdo con las condiciones de configuración recomendadas por el fabricante.
	Debe soportar estándares IEEE aplicables, incluyendo como mínimo 802.11a/b/g/n/ac/ax/be, 802.1Q, 802.1X, 802.3af/at/bt cuando aplique, 802.3az, 802.3bz, y otros equivalentes necesarios para interoperabilidad empresarial.
	Debe soportar WPA2-Enterprise, WPA3-Enterprise o mecanismos equivalentes vigentes, autenticación 802.1X/EAP, cifrado seguro y segmentación por SSID/VLAN. El uso de protocolos obsoletos deberá quedar deshabilitado salvo necesidad justificada de compatibilidad.
	Los equipos deberán cumplir requisitos ambientales y de seguridad aplicables, tales como RoHS, eficiencia energética o certificaciones equivalentes del fabricante, según proceda para el tipo de dispositivo ofertado.
	Debe contar con mecanismos de implementación simplificada o aprovisionamiento automatizado, tales como plantillas, perfiles, descubrimiento automático, Zero Touch Provisioning o funcionalidad equivalente.
	La solución deberá integrarse con controles de seguridad institucionales o propuestos, tales como firewall, NAC, directorio activo, RADIUS/TACACS+, SIEM, filtrado web o control de aplicaciones. Las capacidades podrán ser nativas, licenciadas, integradas o prestadas por soluciones de terceros.
	Debe soportar al menos una modalidad segura de transporte del tráfico inalámbrico hacia la red institucional y permitir conmutación local o modo puente. En caso de soportar túneles centralizados, estos deberán usar mecanismos seguros como IPsec, DTLS, TLS u otros equivalentes.
	Debe soportar administración segura mediante HTTPS/TLS, SSH, SNMPv2c o SNMPv3, registro de eventos, exportación de logs y,

	preferiblemente, API REST o mecanismo documentado para integración con herramientas de monitoreo.
	El punto de acceso deberá soportar operación en escenarios de alta densidad. Como referencia mínima, deberá permitir al menos 512 asociaciones de clientes por punto de acceso o acreditar una capacidad superior según documentación técnica del fabricante.
	Administración centralizada, local o en nube, según diseño aceptado por la entidad
	Soporte para autenticación segura, cifrado vigente, segmentación por SSID, redes de invitados y políticas de acceso
	La oferta deberá incluir todos los accesorios necesarios para instalación y operación, tales como kits de montaje en techo, pared o riel, tornillería, elementos de fijación, documentación y componentes requeridos para puesta en servicio.
	Soporte técnico, garantía y actualizaciones por 36 meses
	El fabricante, integrador o canal deberá acreditar capacidad técnica mediante fichas técnicas, certificaciones, experiencia verificable, documentación pública, centro de soporte, mesa de ayuda o representación comercial. No se exige pertenencia a publicaciones, rankings o categorías comerciales específicas.

La solución SD-LAN deberá permitir integrar un sistema de monitoreo, administración y seguridad del mismo fabricante de los equipos de red, este deberá contar como mínimo con las siguientes funcionalidades:

- Vista absoluta y granular de toda la red, que este en capacidad de monitorear equipos LAN DC, en el caso de LAN y WLAN Campus cuando sea actualizada.
- Gestión del ciclo de vida de los dispositivos y demás componentes de red.
- Gestión de despliegues para nuevos dispositivos ZTP (“Zero Touch Provisioning” por sus siglas en Ingles).
- La solución debe permitir agregar dispositivos de Red de acuerdo con las necesidades de la entidad y así garantizar las capacidades y requerimientos de seguridad para nuevas implementaciones.
- Gestión automatizada de actualizaciones de versión de software de los dispositivos.
- Detección de eventos de seguridad de los equipos y dispositivos conectados mediante Indicadores de compromiso para los componentes de la red LAN, especialmente a futuro en la LAN Y WLAN Campus.
- Entrega de notificaciones sobre eventos anómalos en la red y alertas presentadas en la solución SD-LAN.
- La plataforma de gestión de red debe incluir doble factor de autenticación para los administradores de esta.
- La solución debe contar con La funcionalidad de validación de usuario, permitiendo identificar de manera oportuna aplicaciones usadas, usuarios, comportamiento y uso de La red.
- Debe soportar detección automática de dispositivos, usuarios basados en grupos y asignación dinámica de VLANs y políticas básicas de seguridad.
- Debe permitir configuraciones masivas consistentes mediante plantillas.

- Debe tener la posibilidad de configurar perfiles dinámicos en los puertos de switch de tal forma que la detección automática de un dispositivo (basado en LLDP y atributos de fabricante OUI) permita aplicar el perfil deseado, que debe incluir IoT como mínimo.
- Debe permitir tener visibilidad de los niveles de servicio esperados, tales como throughput, salud del dispositivo, CPU, utilización de memoria, ancho de banda, detección de congestión, utilización de tráfico, bytes transferidos, consumo de potencia.
- Debe poder visualizar el inventario de dispositivos, topología y ubicación.
- La solución de SD-LAN debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica a futuro. Al menos los ataques de denegación de servicio deben ser mitigados por la infraestructura a través del envío de paquetes de des autenticación.
- La solución debe poder segmentar y perfilar los accesos de los diferentes dispositivos dependiendo de la VLAN en la que fue desplegado.
- Debe soportar APIs para integración con terceros como sistemas SIEM, de gestión de casos de atención, antivirus, sistemas de autenticación, SandBox, entre otras.
- La solución debe estar en capacidad de generar reportes tanto de red como de seguridad para su análisis.

Entregables mínimos solicitados
Cronograma de actividades, responsables, ventanas de intervención y metodología de implementación
Diagrama físico y lógico de la solución a implementar
Relación de equipos, seriales, cantidades, ubicación y características principales
Documento que evidencie instalación física, conexión y energización
Documento que detalle configuraciones realizadas, VLAN, puertos, perfiles y parámetros principales
Informe de pruebas de conectividad, segmentación, operación inalámbrica y validación del canal
Copia de configuraciones iniciales y procedimiento básico de restauración
Certificados, licencias (3 años), soportes de garantía y vigencia de soporte por un tiempo mínimo de 3 años
Sesión técnica al equipo de TI de la entidad sobre operación básica, monitoreo y escalamiento
Documentación final y acta de entrega

Organizadores y adecuación física de rack
Organizadores compatibles con rack estándar de 19 pulgadas o infraestructura existente

Peinado, organización, rotulado básico y aseguramiento del cableado asociado a los equipos instalados
Separación ordenada de cableado, identificación de conexiones, reducción de cruces, protección física y facilidad de mantenimiento
Servicios técnicos requeridos
Enrackado, conexión eléctrica, conexión de red y validación física
Instalación en techo o pared, conexión de red y verificación de encendido
Fijación y adecuación de organizadores verticales
Peinado, ordenamiento, identificación básica y aseguramiento de cableado
VLAN, troncales, agregación de enlaces, administración segura, rutas o funciones de capa 3 cuando aplique, respaldo de configuración y pruebas
VLAN de usuario, administración, puertos troncales, puertos de acceso, seguridad básica por puerto, QoS y pruebas
SSID institucionales, segmentación, autenticación, seguridad, canalización básica, potencia y validación de cobertura funcional
SNMP, syslog, alertas básicas o mecanismos equivalentes, según las herramientas disponibles en la entidad
Entrega de copias de configuración inicial, inventario lógico y procedimiento básico de restauración
PRUEBAS - Conectividad, segmentación, acceso a servicios, operación inalámbrica, redundancia básica y validación de enlaces

** *Junto con las solicitudes técnica también se cuenta que dentro de lo solicitado se pueda contar con disposición de RAEE de los equipos electrónicos que van a quedar fuera de funcionamiento, realizando su respectiva clasificación y gestión, garantizando el correcto tratamiento de estos y emitiendo un certificado de la correcta disposición y destrucción de los equipos.*

SERVICIOS PROFESIONALES DE SOPORTE — 24 MESES

El oferente deberá incluir en su propuesta la prestación de Servicios Profesionales de Soporte para la totalidad de los equipos de red referenciados en el presente documento (Switch Core DC y Campus, Switch Acceso DC y Campus, Switch Acceso PoE y Puntos de Acceso Inalámbrico), por un periodo de veinte y cuatro (24) meses contados a partir de la entrega y aceptación formal de los equipos. Los servicios de soporte deberán garantizar la continuidad operativa, la disponibilidad de la infraestructura y la resolución oportuna de incidentes técnicos conforme a los niveles de servicio establecidos.

Solución	Servicios Profesionales de Soporte (24 Meses) — Especificaciones Requeridas
Alcance del Soporte	El servicio deberá cubrir la totalidad de los equipos entregados e instalados en el marco del presente contrato: Switch Core DC y Campus (2 unidades), Switch Acceso DC y Campus (5 unidades), Switch Acceso PoE (1 unidad) y Puntos de Acceso Inalámbrico (6 unidades). El soporte incluirá tanto el hardware como el software de gestión (plataforma SD-LAN) asociados a la solución ofertada.
Modalidad y Horario de Atención	El proveedor deberá garantizar soporte técnico especializado en modalidad presencial y/o remota, disponible 7x24 para atención de fallas críticas (Prioridad Alta). Para incidentes de menor impacto, la atención deberá estar disponible en horario hábil (lunes a viernes, 7:00 a.m. – 6:00 p.m., hora Colombia). Se deberá incluir una mesa de ayuda o canal formal de apertura de casos (teléfono, correo electrónico o portal web).
Acuerdos de Nivel de Servicio (ANS)	**Prioridad Alta (Falla Mayor/Crítica):** Fallas que impiden el funcionamiento total o parcial de la red, generan indisponibilidad de servicios críticos o afectan a múltiples usuarios. Tiempo de respuesta inicial: máximo 4 horas. Tiempo de restauración del servicio: máximo 8 horas hábiles. **Prioridad Media (Falla Leve/Parcial):** Fallas que afectan funcionalidades específicas sin generar indisponibilidad total. Tiempo de respuesta inicial: máximo 8 horas hábiles. Tiempo de resolución: máximo 3 días hábiles. **Prioridad Baja (Consultas y Mejoras):** Solicitudes de orientación, configuraciones menores o generación de reportes. Tiempo de respuesta: máximo 5 días hábiles.
Actividades Mínimas Incluidas	Atención y resolución de incidentes técnicos relacionados con los equipos instalados (hardware y software). Mantenimiento preventivo semestral: revisión de configuraciones, actualización de firmware/software según recomendación del fabricante, verificación de salud de dispositivos y generación de informe técnico. Soporte en la gestión y monitoreo de la plataforma SD-LAN durante el período de vigencia del servicio. Asistencia remota y/o presencial para cambios de configuración, adición de VLANs, ajuste de políticas de seguridad y optimización de rendimiento, cuando sean requeridos por la Entidad. Gestión de escalamiento con el fabricante (soporte Nivel 3 / TAC) cuando la complejidad del incidente así lo requiera. Entrega de informes mensuales de gestión de casos: apertura, estado, resolución, tiempos de atención y cumplimiento de ANS.

Personal Técnico Asignado	El oferente deberá designar al menos un (1) ingeniero de soporte certificado por el fabricante de la solución ofertada, con experiencia mínima de cinco (5) años en administración y soporte de redes LAN/WLAN empresariales. Adicional con (4) años de experiencia especifica en proyectos de seguridad informatica, esta será acredita mediante certificaciones de experiencia laboral. Y debera mostrar las siguientes certificaciones. ☐ **Certified Solution Specialist Network Security** ☐ **Certified Professional Network Security**
Entregables del Servicio	Informe mensual de gestión de incidentes con cumplimiento de ANS. Informe semestral de mantenimiento preventivo con hallazgos, acciones ejecutadas y recomendaciones. Respaldo de configuraciones actualizado posterior a cada cambio o mantenimiento ejecutado. Informe final de cierre del servicio al término de los 24 meses, con consolidado de incidentes, tendencias, disponibilidad promedio y recomendaciones para el siguiente periodo.
Vigencia y Condiciones	El servicio tendrá una vigencia de doce (24) meses contados a partir de la firma del acta de entrega y aceptación definitiva de los equipos. El costo del servicio deberá cotizarse de forma explícita e independiente al valor de los equipos. No se acepta que los servicios profesionales queden incluidos de forma implícita o no cuantificada dentro del precio de los bienes.

REQUISITOS HABILITANTES DEL PROVEEDOR DE SERVICIOS

Los siguientes requisitos son de obligatorio cumplimiento y serán verificados como condiciones habilitantes para la presentación de la propuesta. El incumplimiento de cualquiera de ellos será causal de rechazo de la oferta.

1. El oferente deberá designar al menos un (1) profesional responsable de la coordinación, seguimiento y control del proyecto, con formación de posgrado o especialización en áreas de tecnología, gestión de proyectos tecnológicos o disciplinas afines. Este profesional deberá contar con experiencia mínima de tres (5) años liderando proyectos de implementación de infraestructura tecnológica o servicios de TI. Cualquier

cambio de este recurso durante la ejecución del contrato deberá ser informado y aprobado previamente por la Entidad.

Adicionalmente, el profesional designado deberá acreditar las siguientes certificaciones vigentes, las cuales serán verificadas como requisito habilitante y deberán ser anexadas a la propuesta:

- ITIL V4 Foundation
- Scrum Master (certificación vigente emitida por organismo reconocido)
- ISO/IEC 27001:2022 Auditor Interno
- Project Management Professional — PMP (vigente y emitida por el PMI)
- Certificación del fabricante de la solución ofertada en nivel básico o superior (emitida directamente por el fabricante a nombre del profesional)
- CISM — Certified Information Security Manager (emitida por ISACA, vigente a la fecha de cierre del proceso)

2. El oferente debe contar con una mesa de servicios y/o mesa de ayuda que esté certificada bajo la norma internacional vigente del Sistema de Gestión de Servicios en su versión más reciente, aplicable a los procesos de seguridad y soporte de servicios. Esta certificación asegurará la calidad, gestión y mejora continua de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida directamente al oferente por el ente certificador autorizado.

3. El oferente deberá alinearse a las políticas de seguridad de la entidad, así como el modelo MSPI del Ministerio de las Telecomunicaciones de Colombia – Mintic, el prestador de servicio debe contar con certificación vigente en la norma de estándares internacionales del Sistema de Gestión de Seguridad de la Información en su versión mas reciente para los procesos relacionados con seguridad y mesa de servicios, a fin de garantizar la calidad, gestión y mejora de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.

4. El oferente deberá garantizar que los Servicios Administrados cuente con procedimientos formalmente establecidos, documentados y operativos para la gestión de incidentes de seguridad de la información. Para ello, el oferente deberá contar con certificación vigente en la norma Gestión de

Incidentes de Seguridad de la Información, la cual establece las mejores prácticas para el tratamiento de incidentes en todo su ciclo de vida: preparación, detección, evaluación, respuesta y aprendizaje. Esta certificación respaldará el cumplimiento de estándares internacionales en la gestión de incidentes, conforme a las políticas de seguridad de la entidad y en armonía con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – MinTIC. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.