UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

ESPECIFICACIONES TÉCNICAS
EQUIPOS NETWORKING
PROGRAMA RED UDNET

JULIO DE 2026

Contenido

Especificaciones técnicas

1. Objeto del proceso

Adquirir equipos activos de red switches y access points, incluyendo hardware, licenciamiento, garantía y soporte técnico integral, con el fin de garantizar la disponibilidad, seguridad, escalabilidad y el óptimo rendimiento de los servicios de red en las sedes de la Universidad Distrital Francisco José de Caldas, conforme con las condiciones y especificaciones técnicas establecidas.

2. Alcance técnico

a. Suministrar equipos de red equipos de conmutación (switches) y equipos de puntos de acceso (Access Point) tipo indoor y outdoor, junto con sus respectivos componentes, accesorios, licenciamiento, garantía y soporte.

b. Los equipos a suministrar son los siguientes:

- **i.** Un (1) switch de 24 puertos - Core
- **ii.** Cinco (5) switch de 48 puertos – Datos
- **iii.** Tres (3) switch de 24 puertos – Datos
- **iv.** Un (1) switch de 48 puertos – Multigigabit
- **v.** Dos (2) switch de 24 puertos – Multigigabit
- **vi.** Treinta y cuatro (34) Access point – Indoor
- **vii.** Cuatro (4) Access point – Oudoor

c. Estos equipos deben instalarse e integrarse con la red corporativa de la Universidad, permitiendo brindar conectividad a las diferentes áreas de trabajo y dispositivos en las sedes que la Universidad defina, garantizando alto rendimiento en las comunicaciones de red.

d. Los equipos deben permitir la gestión del acceso a la red mediante la autenticación de usuarios, a través de su integración con la red convergente y con las plataformas Cisco® ISE (NAC) y Cisco® DNA, así como con el directorio activo Microsoft® actualmente implementado en la Universidad.

e. Los equipos, componentes y accesorios adquiridos deberán contar con servicio de licenciamiento, soporte, garantía y reemplazo de partes por un periodo de mínimo tres (3) años, bajo un esquema de atención 8x5xNBD (8 horas diarias, 5 días hábiles a la semana, con reemplazo de hardware al siguiente día hábil), de acuerdo con las condiciones establecidas.

f. Los equipos y componentes objeto del presente proceso deberán soportar los protocolos IPv4 e IPv6. El soporte de IPv6 deberá estar certificado mediante el programa IPv6 Ready Logo.

g. Realizar una transferencia de conocimiento con una duración de doce (12) horas, dirigida al personal técnico designado por la Supervisión, que incluya temas de troubleshooting, administración y gestión de los equipos de la solución LAN–WLAN.

3. Descripción del contexto técnico

La Universidad Distrital Francisco José de Caldas cuenta con una arquitectura de red en topología estrella, en la que convergen 15 sedes del campus universitario a través de una WAN conformada por 15 enlaces dedicados de datos, aprovisionados por el ISP actual. Estos enlaces garantizan la conectividad de toda la comunidad universitaria y permiten el acceso a los diferentes servicios desplegados en la red convergente.

La infraestructura de Networking LAN principalmente está compuesta por equipos de conmutación de la marca Cisco® y algunos equipos de la marca Juniper®, instalados y en operación en las distintas sedes. En el caso de Cisco®, se dispone de switches de las series 9500, 9300, 3750, 2960 entre otros; mientras que, para Juniper®, se cuenta con equipos de las series EX4300, EX4600 y QFX5100.

En cuanto a la infraestructura WLAN, la Universidad tiene desplegadas dos soluciones de red inalámbrica. La primera y en su mayoría del fabricante Cisco®, incluye controladoras de las series C9800, así como Access Point (puntos de acceso) de las series C9120AXI y C9124AXI. La segunda solución, del fabricante Ruckus®, cuenta con controladoras SZ-104 y SZ-124, y puntos de acceso de las series R600, R610 y T300.

Como parte de la estrategia institucional de seguridad y administración de la infraestructura de red, la Universidad cuenta con plataformas especializadas Cisco Identity Services Engine (ISE) para el control de acceso a la red (NAC) y Cisco Catalyst Center para la administración centralizada, automatización, monitoreo, aseguramiento (Assurance), aprovisionamiento y gestión del ciclo de vida de los dispositivos de red.

En este contexto, la tecnología de equipos Cisco® responde a una necesidad técnica de interoperabilidad con la infraestructura actualmente instalada y con las plataformas de gestión existentes. Los equipos Cisco® permiten la integración nativa con Cisco ISE para la aplicación de políticas de autenticación, autorización y control de acceso mediante estándares como IEEE 802.1X, MAB, CoA, TrustSec, profiling de dispositivos y demás funcionalidades de seguridad implementadas institucionalmente. De igual manera, la integración con Cisco Catalyst Center permite mantener las capacidades de automatización, aprovisionamiento Plug and Play (PnP), administración de imágenes de software (SWIM), monitoreo de salud de la red, analítica, telemetría y administración centralizada, funcionalidades que forman parte de la operación actual de la Universidad.

Adicionalmente, dentro del presente proceso se contempla la adquisición de un switch Cisco Catalyst 9500-24Y4C, el cual será instalado en una de las sedes donde actualmente se encuentra en operación un equipo del mismo modelo. Esta adquisición tiene como finalidad conformar una arquitectura de alta disponibilidad (High Availability - HA) mediante la tecnología StackWise Virtual, funcionalidad soportada únicamente entre equipos del mismo modelo y familia tecnológica, permitiendo disponer de redundancia a nivel de plano de control y plano de datos, eliminación de puntos únicos de falla, continuidad operativa durante eventos de mantenimiento o fallas y mayor disponibilidad de los servicios de red que soportan la operación institucional.

En consecuencia, la adquisición de equipos Cisco® no obedece a una preferencia de marca, sino a la necesidad de garantizar la compatibilidad tecnológica, la interoperabilidad con la infraestructura existente, el aprovechamiento de las inversiones previamente realizadas por la Universidad, la continuidad operacional, la seguridad de la red y el cumplimiento de los niveles de disponibilidad requeridos para la prestación de los servicios institucionales.

4. Requerimientos técnicos mínimos obligatorios

a. La totalidad de los equipos activos de red, switches, Access Point, módulos, fuentes, transceptores, componentes y cables de apilamiento, inyectores PoE, antenas propietarias y licencias, deberán ser de la misma marca y estar oficialmente soportados para la referencia ofertada. La obligación no se extiende a elementos pasivos o auxiliares como cableado Categoría 6A, patch cords, conectores, jacks, patch panels, pasamuros, pasaplacas, guayas, canaletas, tornillería, anclajes y herrajes. Estos podrán ser de terceros siempre que sean nuevos, certificados, compatibles, cumplan las especificaciones técnicas, no reduzcan el rendimiento ni la capacidad PoE y no afecten la garantía o soporte oficial de los equipos.

b. Los productos adquiridos deberán ser nuevos, originales, ensamblados en fábrica y registrados a nombre de la Universidad Distrital Francisco José de Caldas. Los equipos deberán entregarse en sus empaques originales, debidamente sellados. La Universidad, a través de la supervisión, verificará en todo momento el cumplimiento de las condiciones de originalidad y estado de los equipos y/o componentes adquiridos en el marco del presente proceso.

c. Todos los equipos deberán entregarse con la última versión de software disponible y estable al momento de la entrega. Durante la vigencia del servicio de soporte y licenciamiento, deberán actualizarse a las versiones estables que libere el fabricante, previa autorización de la supervisión o quien la supervisión designe.

d. Para cada equipo se deberán contemplar todos los accesorios, cables de poder, módulos, licenciamiento y demás componentes necesarios para su instalación, puesta en funcionamiento e integración con las plataformas existentes de la Universidad, tales como Cisco® ISE (Identity Services Engine) y Cisco® DNA (Digital Network Architecture).

e. El Switch Core deberá integrarse con el appliance Cisco® DNA (Digital Network Architecture) versión 2.3.7.7 y el controlador de acceso a la red Cisco® ISE (Identity Services Engine) a efectos de aprovechar los recursos, tecnologías y plataformas de administración de la Universidad, por lo tanto, el proponente debe suministrar las licencias nivel Avanzado necesarias para el equipo switch core sobre la plataforma DNA e ISE, las cuales deben estar contempladas en la oferta económica.

f. Todos los switches de acceso deberán integrarse con el appliance Cisco® DNA (Digital Network Architecture) versión 2.3.7.7 y el controlador de acceso a la red Cisco® ISE (Identity Services Engine) a efectos de aprovechar los recursos, tecnologías y plataformas de administración de la Universidad, por lo tanto, el proponente debe suministrar las licencias nivel Esencial necesarias para los equipos switches sobre la plataforma DNA e ISE, las cuales deben estar contempladas en la oferta económica.

g. Todos los Access Point deberán integrarse con la controladora WLC Cisco 9800, appliance Cisco® DNA (Digital Network Architecture) versión 2.3.7.7 y el controlador de acceso a la red Cisco® ISE (Identity Services Engine) a efectos de aprovechar los recursos, tecnologías y plataformas de administración de la Universidad, por lo tanto, el proponente debe suministrar las licencias nivel

Avanzado necesarias para los Access Point sobre la plataforma DNA e ISE, las cuales deben estar contempladas en la oferta económica.

h. El proponente debe contemplar los pasamuros, pasaplacas y perforaciones pertinentes para la correcta instalación de los Access Point.

i. El proponente deberá considerar que los Access Point serán instalados en las ubicaciones que determine la Universidad. Para los Access Point Indoor se utilizará prioritariamente el cableado estructurado y los puntos de red existentes; por tanto, no se deberá contemplar el suministro ni la instalación de nuevos tendidos de cableado, salvo que la Supervisión identifique y autorice expresamente una adecuación excepcional. Para los Access Point Outdoor, el proponente deberá incluir el suministro, instalación, terminación, etiquetado y certificación de un enlace de cableado estructurado Categoría 6A por cada equipo, con una longitud máxima de noventa (90) metros de enlace permanente, medida desde el patch panel hasta la salida de telecomunicaciones o punto de conexión del Access Point. Adicionalmente, para todos los Access Point se deberán incluir los materiales, herramientas, soportes, anclajes, guayas, pasamuros, pasaplacas, elementos de protección, accesorios y demás componentes necesarios para su correcta instalación, así como el licenciamiento, soporte, garantía, módulos e inyectores PoE requeridos, en cumplimiento de las condiciones técnicas exigidas.

j. Los Access Point deberán incluir un inyector PoE Multigigabit, nuevo, original y oficialmente compatible con la referencia ofertada, con potencia suficiente para garantizar el funcionamiento integral del equipo. No se aceptarán inyectores que ocasionen modos de potencia reducida, deshabiliten o limiten radios, cadenas espaciales, interfaces o funcionalidades exigidas. Cuando el equipo requiera IEEE 802.3bt o un nivel superior a IEEE 802.3at para su operación plena, el inyector deberá suministrar dicho nivel de potencia y mantener la velocidad Multigigabit requerida. La compatibilidad y capacidad deberán acreditarse mediante documentación oficial del fabricante.

k. Para la conformación de la solución StackWise Virtual entre el nuevo switch Core y el switch Cisco Catalyst 9500-24Y4C actualmente instalado en la Universidad, se utilizarán puertos de 40/100 Gigabit Ethernet compatibles con interfaces QSFP+/QSFP28. El contratista deberá suministrar todos los cables, módulos, transceptores y demás accesorios necesarios para ambos extremos de los enlaces StackWise Virtual Link, SVL, y Dual-Active Detection, DAD, tanto para el equipo Core existente como para el nuevo equipo.

l. Los Access Point Indoor y Outdoor ofertados deberán corresponder a referencias cuyo dominio regulatorio se encuentre oficialmente aprobado para su comercialización y operación en Colombia, de conformidad con las bandas de frecuencia, canales y niveles de potencia autorizados. El proponente deberá acreditar esta condición mediante documentación oficial del fabricante o mediante los mecanismos oficiales de consulta regulatoria dispuestos por este, identificando como mínimo el fabricante, modelo, PID completo, país de operación, dominio regulatorio y estado de aprobación. No será suficiente presentar únicamente la ficha técnica general de la familia cuando esta no permita verificar la autorización específica del PID ofertado para Colombia

Así mismo se presentan los requerimientos por cada tipo de equipos:

4.1. Requerimientos técnicos Switch Core

El equipo switch core a adquirir deberá cumplir con lo definido en la "*Tabla 1. Requerimientos técnicos Switch Core 24P*"

REQUERIMIENTOS TÉCNICOS SWITCH CORE 24P	
Ítem	**Descripción**
1	Debe tener mínimo 24 puertos Non-Blocking para conector LC de fibra multimodo a 1/10/25 Gbps con negociación automática (SFP/SFP+/SFP28)
2	Debe tener mínimo 4 puertos 40/100 GE (QSFP+/QSFP28) para uplinks de alta velocidad.
3	Debe soportar configuraciones de apilamiento virtual, que permita unificar mínimo dos (2) unidades de switches de Core como si fueran el mismo switch lógico.
4	Debe permitir configurar, soportar e incluir las licencias para habilitar o configurar los protocolos: • OSPFv3 • VRRPv3 • BGPv4 • ARP • IGMPv3 • SNMPv3 • DHCP Server • DHCP relay • NTP • Enrutamiento estático • Enrutamiento virtual (VRF) • EVPN con VXLAN • SSH v2 • ACL (IPv4 e IPv6)
5	DRAM mínima 16 GB.
6	FLASH mínima 16 GB.
7	El equipo debe ser "*non-blocking*", esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresubscripción, es decir que el equipo soporte mínimo 2.0 Tbps en switching capacity.
8	Los equipos deben poder realizar apilamiento (agrupación o chasis virtual) por medio de cable y módulos propios del fabricante requeridos para su correcto funcionamiento y deberán ser incluidos.
9	Soportar mínimo 32000 direcciones MAC.
10	Soportar mínimo 16000 rutas Multicast IPv4 y mínimo 16000 rutas Multicast IPv6.
11	Soporte de Dual stack para IPv4/IPv6
12	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.
13	Debe soportar las siguientes funcionalidades de enrutamiento para multicast en IPv6: • Protocol Independent Multicast • PIM in Source Specific Multicast (PIM-SSM)
14	Soportar mínimo 64000 rutas IPv4 ARP
15	Soportar mínimo 4000 VLAN ID.
16	Debe soportar Jumbo frame mínimo de 9000 bytes.

REQUERIMIENTOS TÉCNICOS SWITCH CORE 24P	
Ítem	**Descripción**
17	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 900 Mpps.
18	Debe cumplir con los siguientes RFC, funcionalidades y estándares: • RFC2460 (IPv6 Basic specification) • RFC4291 (IPv6 Addressing Architecture) • RFC3484 (Default Address Selection) • RFC4193 (Unique Local IPv6 Unicast Addresses (ULA)) • RFC4443 (ICMPv6) • RFC4862 (SLAAC) • RFC3810 (Multicast Listener Discovery Version 2 (MLDv2) for IPv6) • RFC2711 (Router-Alert option) • RFC1981 (Path MTU Discovery) • RFC4861 (Neighbor Discovery) • RFC5095 (Deprecation of Type 0 Routing Headers in IPv6) • RFC3315 (DHCPv6 filtering) • RFC4861 (Dynamic *"IPv6 Neighbor solicitation/advertisement"* inspection / Neighbor Unreachability Detection filtering) • RFC4862 (IPv6 Stateless Address Autoconfiguration) • OSPFv3: RFC5340, RFC4552 y RFC 5838 • |IEEE 802.1AB LLDP • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.1s RSTP • IEEE 802.1w • IEEE 802.1x • IEEE 802.3ad LACP • IEEE 802.3x
19	El equipo deberá soportar capacidades de generación y exportación de flujos, telemetría o metadatos aplicables al análisis de amenazas de seguridad, incluyendo Flexible NetFlow y Encrypted Traffic Analytics, ETA, cuando esta funcionalidad se encuentre disponible para la referencia ofertada. El equipo deberá permitir su integración futura con una plataforma Cisco especializada de analítica y seguridad para apoyar el análisis de comportamientos relacionados con ataques de comando y control, ransomware, DDoS, malware desconocido, amenazas internas y tráfico cifrado.
20	El equipo debe ser administrado a través de CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder de mínimo 650 W cada una y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 300000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.

REQUERIMIENTOS TÉCNICOS SWITCH CORE 24P	
Ítem	**Descripción**
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: • Implementación automatizada tipo Zero-Touch • Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analíticas y Telemetría. • Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6). • Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	El equipo debe poderse montar en racks de 19 pulgadas e incluir los herrajes para su montaje.
29	Debe incluir cable de conexión y accesorios para apilamiento
30	Los equipos deberán instalarse en configuración de stack (apilamiento), mediante tecnología Stackwise con la solución de Switch Core Cisco Catalyst 9500-24Y4C de la Universidad quedando un único equipo lógico el cual deberá ser administrando y gestionado por una única IP.

Tabla 1. Requerimientos técnicos Switch Core 24P

4.2. Requerimientos técnicos switch acceso multigigabit 48 Puertos

Los equipos switch de acceso multigigabit de 48 puertos a adquirir deberán cumplir con lo definido en la "*Tabla 2. Requerimientos técnicos switch acceso 48 puertos multigigabit*"

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS MULTIGIGABIT	
Ítem	**Descripción**
1	Debe tener mínimo 48 puertos Non-Blocking para conector RJ-45 autosensing 10/100/1000 o 100/1000 MDIX con PoE de 1100W de los cuales mínimo 12 deben ser Multigigabit 100/1G/2,5G/5G
2	Debe tener mínimo 4 puertos de uplink a 10G SFP+ para uplinks de alta velocidad
3	Deben soportar configuraciones de apilamiento de mínimo 8 equipos (entre Switches de Acceso de la misma familia) y se debe tener gestión de los mismos por medio de una única dirección ip
4	Debe soportar los siguientes protocolos: • OSPFv3 • VRRPv3 • BGPv4 • ARP • IGMPv3 • SNMPv3 • DHCP Server • DHCP relay • NTP • Enrutamiento estático • Enrutamiento virtual (VRF) • EVPN con VXLAN • SSH v2 • ACL (IPv4 e IPv6)
5	DRAM mínima 8GB
6	FLASH mínimo 16GB

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS MULTIGIGABIT	
Ítem	**Descripción**
7	El equipo debe ser "*non-blocking*", esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresubscripción, es decir que el equipo soporte mínimo 370 Gbps en switching capacity, sin contar el throughput del módulo físico de stack.
8	El switching capacity del stacking debe ser físico de mínimo 700 Gbps, que permita tener hasta 8 miembros.
9	Soportar mínimo 32.000 direcciones MAC
10	Soportar mínimo 32000 rutas IPv4 ARP plus learned routes – (24,000 directas y 8,000 indirectas)
11	Soportar mínimo 16000 rutas de enrutamiento en IPv6
12	Soporte de Dual stack para IPv4/IPv6
13	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.
14	Soportar mínimo 4000 VLAN ID
15	Debe soportar Jumbo frame mínimo de 9100 bytes
16	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 270 Mpps.
17	Debe cumplir con los siguientes RFC, funcionalidades y estándares: • RFC2460 (IPv6 Basic specification) • RFC4291 (IPv6 Addressing Architecture) • RFC3484 (Default Address Selection) • RFC4193 (Unique Local IPv6 Unicast Addresses (ULA)) • RFC4443 (ICMPv6) • RFC4862 (SLAAC) • RFC1981 (Path MTU Discovery) • RFC4861 (Neighbor Discovery) • RFC3810 (Multicast Listener Discovery version 2 (MLDv2) for IPv6) • RFC2711 (Router-Alert option) • RFC5095 (Deprecation of Type 0 Routing Headers in IPv6) • RFC3315 (DHCPv6 filtering) • RFC4862 IPv6 Stateless Address Autoconfiguration • OSPFv3: RFC5340, RFC4552 y RFC 5838 • IEEE 802.1s • IEEE 802.1w • IEEE 802.1x • IEEE 802.3ad • IEEE 802.3af • IEEE 802.3at • IEEE 802.3x full dúplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification.
18	El equipo deberá soportar capacidades de generación y exportación de flujos, telemetría o metadatos aplicables al análisis de amenazas de seguridad, incluyendo Flexible NetFlow y Encrypted Traffic Analytics, ETA, cuando esta funcionalidad se encuentre disponible para la referencia ofertada. El equipo

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS MULTIGIGABIT	
Ítem	**Descripción**
	deberá permitir su integración futura con una plataforma Cisco especializada de analítica y seguridad para apoyar el análisis de comportamientos relacionados con ataques de comando y control, ransomware, DDoS, malware desconocido, amenazas internas y tráfico cifrado
19	El equipo debe poderse montar en racks de 19 pulgadas e incluir los herrajes para su montaje.
20	El equipo debe ser administrado a través de: CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC. La configuración conjunta de las dos (2) fuentes instaladas deberá proporcionar un presupuesto PoE efectivamente disponible para los puertos del equipo igual o superior a 1100 W, una vez atendido el consumo interno requerido para la operación del switch.
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 270000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: • Implementación automatizada tipo Zero-Touch • Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analíticas y Telemetría. • Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6). • Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	Debe incluir cable y accesorios para apilamiento de mínimo 1 metro.

Tabla 2. Requerimientos técnicos switch acceso 48 puertos multigigabit

4.3. Requerimientos técnicos switch acceso multigigabit 24 puertos

Los equipos switch de acceso multigigabit de 24 puertos a adquirir deberán cumplir con lo definido en la "*Tabla 3. Requerimientos técnicos switch acceso 24 puertos multigigabit*"

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 24 PTS MULTIGIGABIT	
Ítem	**Descripción**
1	Debe tener mínimo 24 puertos Non-Blocking para conector RJ-45 autosensing 10/100/1000 o 100/1000 MDIX con PoE de 1100W de los cuales mínimo 8 deben ser Multigigabit 100/1G/2,5G/5G
2	Debe tener mínimo 4 puertos de uplink a 10G SFP+ para uplinks de alta velocidad
3	Deben soportar configuraciones de apilamiento de mínimo 8 equipos (entre Switches de Acceso de la misma familia) y se debe tener gestión de los mismos por medio de una única dirección ip
4	Debe soportar los siguientes protocolos: • OSPFv3 • VRRPv3 • BGPv4

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 24 PTS MULTIGIGABIT	
Ítem	**Descripción**
	• ARP • IGMPv3 • SNMPv3 • DHCP Server • DHCP relay • NTP • Enrutamiento estático • Enrutamiento virtual (VRF) • EVPN con VXLAN • SSH v2 • ACL (IPv4 e IPv6)
5	DRAM mínima 8GB
6	FLASH mínimo 16GB
7	El equipo debe ser "*non-blocking*", esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresubscripción, es decir que el equipo soporte mínimo 270 Gbps en switching capacity, sin contar el throughput del módulo físico de stack.
8	El switching capacity del stacking debe ser físico de mínimo 580 Gbps, que permita tener hasta 8 miembros.
9	Soportar mínimo 32.000 direcciones MAC
10	Soportar mínimo 32000 rutas IPv4 ARP plus learned routes – (24,000 directas y 8,000 indirectas)
11	Soportar mínimo 16000 rutas de enrutamiento en IPv6
12	Soporte de Dual stack para IPv4/IPv6
13	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.
14	Soportar mínimo 4000 VLAN ID
15	Debe soportar Jumbo frame mínimo de 9100 bytes
16	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 200 Mpps.
17	Debe cumplir con los siguientes RFC, funcionalidades y estándares: • RFC2460 (IPv6 Basic specification) • RFC4291 (IPv6 Addressing Architecture) • RFC3484 (Default Address Selection) • RFC4193 (Unique Local IPv6 Unicast Addresses (ULA)) • RFC4443 (ICMPv6) • RFC4862 (SLAAC) • RFC1981 (Path MTU Discovery) • RFC4861 (Neighbor Discovery) • RFC3810 (Multicast Listener Discovery version 2 (MLDv2) for IPv6) • RFC2711 (Router-Alert option) • RFC5095 (Deprecation of Type 0 Routing Headers in IPv6) • RFC3315 (DHCPv6 filtering) • RFC4862 IPv6 Stateless Address Autoconfiguration • OSPFv3: RFC5340, RFC4552 y RFC 5838 • IEEE 802.1s • IEEE 802.1w • IEEE 802.1x

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 24 PTS MULTIGIGABIT	
Ítem	**Descripción**
	• IEEE 802.3ad • IEEE 802.3af • IEEE 802.3at • IEEE 802.3x full dúplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification.
18	El equipo deberá soportar capacidades de generación y exportación de flujos, telemetría o metadatos aplicables al análisis de amenazas de seguridad, incluyendo Flexible NetFlow y Encrypted Traffic Analytics, ETA, cuando esta funcionalidad se encuentre disponible para la referencia ofertada. El equipo deberá permitir su integración futura con una plataforma Cisco especializada de analítica y seguridad para apoyar el análisis de comportamientos relacionados con ataques de comando y control, ransomware, DDoS, malware desconocido, amenazas internas y tráfico cifrado
19	El equipo debe poderse montar en racks de 19 pulgadas e incluir los herrajes para su montaje.
20	El equipo debe ser administrado a través de: CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC. La configuración conjunta de las dos (2) fuentes instaladas deberá proporcionar un presupuesto PoE efectivamente disponible para los puertos del equipo igual o superior a 1100 W, una vez atendido el consumo interno requerido para la operación del switch.
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 310000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: • Implementación automatizada tipo Zero-Touch • Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analíticas y Telemetría. • Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6). • Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	Debe incluir cable y accesorios para apilamiento de mínimo 1 metro.

Tabla 3. Requerimientos técnicos switch acceso 24 puertos multigigabit

4.4. Requerimientos técnicos switch acceso data 48 puertos

Los equipos switch de acceso de data de 48 puertos a adquirir deberán cumplir con lo definido en la "*Tabla 4. Requerimientos técnicos switch de acceso 48 puertos Data*"

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS DATA	
ítem	**Descripción**
1	Debe tener mínimo 48 puertos Non-Blocking para conector RJ-45 autosensing 10/100/1000 o 100/1000 MDIX.
2	Debe tener mínimo 4 puertos de uplink a 10G SFP+ para uplinks de alta velocidad
3	Deben soportar configuraciones de apilamiento de mínimo 8 equipos (entre Switches de Acceso de la misma familia) y se debe tener gestión de los mismos por medio de una única dirección ip
4	Debe soportar los siguientes protocolos: • OSPFv3 • VRRPv3 • BGPv4 • ARP • IGMPv3 • SNMPv3 • DHCP Server • DHCP relay • NTP • Enrutamiento estático • Enrutamiento virtual (VRF) • EVPN con VXLAN • SSH v2 • ACL (IPv4 e IPv6)
5	DRAM mínima 8GB
6	FLASH mínimo 16GB
7	El equipo debe ser "*non-blocking*", esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresubscripción, es decir que el equipo soporte mínimo 170 Gbps en switching capacity, sin contar el throughput del módulo físico de stack.
8	El switching capacity del stacking debe ser físico de mínimo 480 Gbps, que permita tener hasta 8 miembros.
9	Soportar mínimo 32.000 direcciones MAC
10	Soportar mínimo 32000 rutas IPv4 ARP plus learned routes) – (24,000 directas y 8,000 indirectas)
11	Soportar mínimo 16000 rutas de enrutamiento en IPv6
12	Soporte de Dual stack para IPv4/IPv6
13	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.
14	Soportar mínimo 4000 VLAN ID
15	Debe soportar Jumbo frame mínimo de 9100 bytes
16	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 120 Mpps.
17	Debe cumplir con los siguientes RFC, funcionalidades y estándares: • RFC2460 (IPv6 Basic specification) • RFC4291 (IPv6 Addressing Architecture) • RFC3484 (Default Address Selection) • RFC4193 (Unique Local IPv6 Unicast Addresses (ULA)) • RFC4443 (ICMPv6) • RFC4862 (SLAAC) • RFC1981 (Path MTU Discovery)

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS DATA	
ítem	**Descripción**
	• RFC4861 (Neighbor Discovery) • RFC3810 (Multicast Listener Discovery version 2 (MLDv2) for IPv6) • RFC2711 (Router-Alert option) • RFC5095 (Deprecation of Type 0 Routing Headers in IPv6) • RFC3315 (DHCPv6 filtering) • RFC4862 IPv6 Stateless Address Autoconfiguration • OSPFv3: RFC5340, RFC4552 y RFC 5838 • IEEE 802.1s • IEEE 802.1w • IEEE 802.1x • IEEE 802.3ad • IEEE 802.3x full dúplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification.
18	El equipo deberá soportar capacidades de generación y exportación de flujos, telemetría o metadatos aplicables al análisis de amenazas de seguridad, incluyendo Flexible NetFlow y Encrypted Traffic Analytics, ETA, cuando esta funcionalidad se encuentre disponible para la referencia ofertada. El equipo deberá permitir su integración futura con una plataforma Cisco especializada de analítica y seguridad para apoyar el análisis de comportamientos relacionados con ataques de comando y control, ransomware, DDoS, malware desconocido, amenazas internas y tráfico cifrado.
19	El equipo debe poderse montar en racks de 19 pulgadas e incluir los herrajes para su montaje.
20	El equipo debe ser administrado a través de: CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder de mínimo 350 W cada una y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 370000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: • Implementación automatizada tipo Zero-Touch • Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analíticas y Telemetría. • Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6). • Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	Debe incluir cable y accesorios para apilamiento de mínimo 1 metro.

Tabla 4. Requerimientos técnicos switch de acceso 48 puertos Data

4.5. Requerimientos técnicos switch acceso data 24 puertos

Los equipos switch de acceso de data de 24 puertos a adquirir deberán cumplir con lo definido en la "*Tabla 5. Requerimientos técnicos switch de acceso 24 puertos Data*"

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 24 PTS DATA	
ítem	**Descripción**
1	Debe tener mínimo 24 puertos Non-Blocking para conector RJ-45 autosensing 10/100/1000 o 100/1000 MDIX.
2	Debe tener mínimo 4 puertos de uplink a 10G SFP+ para uplinks de alta velocidad
3	Deben soportar configuraciones de apilamiento de mínimo 8 equipos (entre Switches de Acceso de la misma familia) y se debe tener gestión de los mismos por medio de una única dirección ip
4	Debe soportar los siguientes protocolos: • OSPFv3 • VRRPv3 • BGPv4 • ARP • IGMPv3 • SNMPv3 • DHCP Server • DHCP relay • NTP • Enrutamiento estático • Enrutamiento virtual (VRF) • EVPN con VXLAN • SSH v2 • ACL (IPv4 e IPv6)
5	DRAM mínima 8GB
6	FLASH mínimo 16GB
7	El equipo debe ser "*non-blocking*", esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresubscripción, es decir que el equipo soporte mínimo 120 Gbps en switching capacity, sin contar el throughput del módulo físico de stack.
8	El switching capacity del stacking debe ser físico de mínimo 420 Gbps, que permita tener hasta 8 miembros.
9	Soportar mínimo 32.000 direcciones MAC
10	Soportar mínimo 32000 rutas IPv4 ARP plus learned routes) – (24,000 directas y 8,000 indirectas)
11	Soportar mínimo 16000 rutas de enrutamiento en IPv6
12	Soporte de Dual stack para IPv4/IPv6
13	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.
14	Soportar mínimo 4000 VLAN ID
15	Debe soportar Jumbo frame mínimo de 9100 bytes
16	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 90 Mpps.
17	Debe cumplir con los siguientes RFC, funcionalidades y estándares: • RFC2460 (IPv6 Basic specification)

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 24 PTS DATA	
ítem	**Descripción**
	• RFC4291 (IPv6 Addressing Architecture) • RFC3484 (Default Address Selection) • RFC4193 (Unique Local IPv6 Unicast Addresses (ULA)) • RFC4443 (ICMPv6) • RFC4862 (SLAAC) • RFC1981 (Path MTU Discovery) • RFC4861 (Neighbor Discovery) • RFC3810 (Multicast Listener Discovery version 2 (MLDv2) for IPv6) • RFC2711 (Router-Alert option) • RFC5095 (Deprecation of Type 0 Routing Headers in IPv6) • RFC3315 (DHCPv6 filtering) • RFC4862 IPv6 Stateless Address Autoconfiguration • OSPFv3: RFC5340, RFC4552 y RFC 5838 • IEEE 802.1s • IEEE 802.1w • IEEE 802.1x • IEEE 802.3ad • IEEE 802.3x full dúplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification.
18	El equipo deberá soportar capacidades de generación y exportación de flujos, telemetría o metadatos aplicables al análisis de amenazas de seguridad, incluyendo Flexible NetFlow y Encrypted Traffic Analytics, ETA, cuando esta funcionalidad se encuentre disponible para la referencia ofertada. El equipo deberá permitir su integración futura con una plataforma Cisco especializada de analítica y seguridad para apoyar el análisis de comportamientos relacionados con ataques de comando y control, ransomware, DDoS, malware desconocido, amenazas internas y tráfico cifrado
19	El equipo debe poderse montar en racks de 19 pulgadas e incluir los herrajes para su montaje.
20	El equipo debe ser administrado a través de: CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder de mínimo 350 W cada una y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 370000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: • Implementación automatizada tipo Zero-Touch

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 24 PTS DATA	
ítem	**Descripción**
	• Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analíticas y Telemetría. • Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6). • Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	Debe incluir cable y accesorios para apilamiento de mínimo 1 metro.

Tabla 5. Requerimientos técnicos switch de acceso 24 puertos Data

4.6. Requerimientos técnicos Access Point Indoor

Los equipos Access point indoor a adquirir deberán cumplir con lo definido en la "*Tabla 6. Requerimientos Técnicos Access Point Indoor*"

REQUERIMIENTOS TÉCNICOS ACCESS POINT INDOOR	
Ítem	**Descripción**
1	Debe cumplir los estándares de comunicación Wifi a/b/g/n/ac/ax
2	Debe funcionar en las bandas de frecuencia 2.4 GHz, 5 GHz y 6 GHz.
3	Debe soportar mínimo el siguiente ancho de banda en los siguientes estándares: • 802.11be • 802.11ax • 802.11ac • 802.11n versión 2.0
4	Debe soportar IPv4, IPv6, dual-stack a nivel de hardware y software.
5	La cobertura del AP debe ser omnidireccional.
6	Debe soportar como mínimo una configuración 2x2:2 en 2,4 GHz, 4x4:4 en 5 GHz y 4x4:4 en 6 GHz, con MU-MIMO conforme con las capacidades oficialmente soportadas por el fabricante
7	Debe soportar beamforming o beamflex
8	Debe contar con antenas internas únicamente
9	Debe poder realizar un análisis de espectro de RF avanzado a través del Access Point o mediante la Controladora Inalámbrica con el fin de aprovechar tecnologías como Wireless Intrusion Prevention System (wIPS) y Dynamic Frequency Selection o ChannelFly.
10	Debe ser administrable por CLI (SSH), SNMPv1, 2, 3 y Vía equipo Controlador.
11	Debe soportar alimentación PoE sobre el estándar 802.3at.
12	Debe contar con mínimo un (1) puerto RJ-45 auto MDI/X, auto-sensing (100/1000/2500/5000 BASE-T)
13	Rango de temperaturas mínimas en operación 0°C a 50°C
14	Condiciones de humedad mínimas 10% a 90% sin condensación (noncondensing)
15	Debe soportar WPA, WPA2, WPA3
16	Debe cumplir con la certificación generada por la WIFI ALLIANCE para Wi-Fi 7 (R1), Wi-Fi 6 (R2), Wi-Fi 6E, WPA3-R3, WPA3-Suite B, Enhanced Open Security

Tabla 6. Requerimientos Técnicos Access Point Indoor

4.7. Requerimientos técnicos Access Point Outdoor

Los equipos Access point outdoor a adquirir deberán cumplir con lo definido en la "*Tabla 7~~8~~. Requerimientos Técnicos Access Point Outdoor*"

REQUERIMIENTOS TÉCNICOS ACCESS POINT OUTDOOR	
Ítem	**Descripción**
1	Debe cumplir los estándares de comunicación Wifi a/b/g/n/ac/ax
2	Debe funcionar en las bandas de frecuencia 2.4 GHz y 5 GHz
3	Debe soportar mínimo el siguiente ancho de banda en los siguientes estándares: • 802.11n versión 2.0 • 802.11ac • 802.11ax
4	Debe soportar IPv4, IPv6
5	La cobertura del AP debe ser omnidireccional.
6	Debe soportar operación simultánea en las bandas de 2,4 GHz y 5 GHz, con una configuración mínima 4x4:4 y MU-MIMO en cada banda conforme con las capacidades oficialmente soportadas por el fabricante
7	Debe soportar beamforming o beamflex
8	Debe contar con cuatro (4) antenas externas
9	Debe poder realizar un análisis de espectro de RF avanzado a través del Access Point o mediante la Controladora Inalámbrica con el fin de aprovechar tecnologías como Wireless Intrusion Prevention System (wIPS) y Dynamic Frequency Selection o ChannelFly.
10	Debe ser administrable por CLI (SSH), SNMPv1, 2, 3 y Vía equipo Controlador
11	Debe soportar alimentación PoE sobre el estándar 802.3at
12	Debe contar con mínimo un (1) puerto RJ-45 auto MDI/X, auto-sensing (100/1000/2500 BASE-T)
13	Rango de temperaturas mínimas -40°C a 65°C
14	Condiciones de humedad mínimas 0% a 100% con condensación (condensing)
15	Debe soportar el estándar IP67
16	Debe soportar WPA, WPA2, WPA3
17	Debe cumplir con la certificación generada por la WIFI ALLIANCE para Wi-Fi 6

Tabla 7. Requerimientos Técnicos Access Point Outdoor

4.8. Ubicación de los equipos

La distribución relacionada a continuación corresponde a una ubicación preliminar de los equipos objeto del contrato. La Universidad se reserva la facultad de ajustar la sede, edificio, bloque, piso o área de instalación durante la adjudicación o la ejecución contractual, atendiendo las necesidades del servicio y las condiciones técnicas y operativas de la infraestructura institucional. La distribución definitiva será establecida y comunicada por la Supervisión antes de la instalación de cada equipo.

Ítem	Tipo de dispositivo	Sede	Espacio	Cantidad
1	Access Point Indoor	Aduanilla de Paiba	Edificio Sanz, Central e Investigadores	34
2	Access Point Outdoor	Aduanilla de Paiba	Edificio Sanz y Central	4
3	Switch Core	Bosa	DC	1
4	Switch Multigigabit 48 Puertos	Aduanilla de Paiba	Sanz	1
5	Switch Datos 48 Puertos	Aduanilla de Paiba	Central	1
6	Switch Datos 48 Puertos	Aduanilla de Paiba	Investigadores	1
7	Switch Multigigabit 24 Puertos	Macarena A	TR1	1
8	Switch Datos 24 Puertos	Macarena A	TR2	1
9	Switch Datos 48 Puertos	Calle 40	Sabio P6	2
10	Switch Multigigabit 24 Puertos	Calle 40	Sabio P6	1
11	Switch Datos 24 Puertos	Vivero	Cartografia	1
12	Switch Datos 24 Puertos	Vivero	Coordinación	1
13	Switch Datos 48 Puertos	Vivero	Microbiologia	1

Tabla 8 - Distribución preliminar de los equipos

5. Garantía y soporte

Todos y cada uno de los equipos a suministrar deben contar con un periodo de garantía y soporte de mínimo tres (3) años, bajo las siguientes condiciones:

5.1. Garantía: Se entiende como la obligación del contratista de asegurar el correcto funcionamiento de los equipos, componentes y elementos asociados a la infraestructura LAN y WLAN**.** La garantía cubrirá defectos de funcionamiento, errores asociados a la implementación de la solución y fallas en los componentes de software suministrados, así como en los componentes físicos, licenciamiento y demás elementos que hagan parte de la solución, asegurando su corrección sin costo adicional para la entidad.

El contratista deberá garantizar la reposición o sustitución de componentes físicos defectuosos (hardware) sin costo para la Universidad, cuando la falla sea atribuible a defectos de fabricación, configuración o funcionamiento de la solución suministrada.

Cuando el diagnóstico sobre los equipos o partes determine falla total o parcial, el contratista deberá realizar el proceso de RMA, coordinar la logística y realizar la instalación configuración y puesta en correcto funcionamiento del equipo a reemplazar, así como la devolución del equipo o parte afectada durante el tiempo de garantía vigente.

Todo traslado de equipos y elementos estará a cargo del contratista, tanto para el retiro como para la entrega en las instalaciones de la Universidad.

En caso de falla el contratista proporcionará y dejará en funcionamiento un sustituto de características y capacidades iguales o superiores, (incluyendo sus componentes), sin que ello genere costos adicionales para la Universidad Distrital Francisco José de Caldas.

La atención de soporte y reemplazo de partes será en esquema 8x5xNBD: 5 días hábiles de la semana de 8:00 am a 5:00 pm, con remplazo de hardware al siguiente día hábil. Estos servicios hacen parte de la oferta incluyendo todos costos asociados para su cumplimiento (fletes, impuestos, transporte, importación, entre otros).

5.2. Soporte y mantenimiento: Son todas las actividades y procedimientos que conlleven a la atención de requerimientos técnicos solicitados a los equipos LAN y WLAN, para atender eventos o incidencias que se presenten.

El soporte a contratar debe ser de partner con certificación vigente de la marca de los equipos, este soporte iniciará a partir de la entrega de los equipos en correcto funcionamiento, con las respectivas pruebas de arranque y recibo a satisfacción por parte del supervisor, debe incluir la última versión oficial y estable del software y firmware, lo cual debe ser realizado por el personal técnico certificado por el fabricante. Por lo tanto, el contratista debe asegurar que cuenta con este personal en cumplimento de términos y condiciones establecidas por la Universidad.

El contratista deberá garantizar el correcto funcionamiento de la solución de networking a nivel de red durante el periodo de garantía y soporte, asegurando la operación continua de todos los componentes suministrados.

Se debe contar con los siguientes niveles de atención durante el periodo de la duración del contrato:

- **i.** Atención telefónica y/o atención vía correo electrónico a través de Centro de atención de llamadas o de medios electrónicos: Atención telefónica y/o de correo electrónico inmediata en esquema 8X5XNBD para reportar la falla.
- **ii.** Atención remota: Soporte remoto en horario hábil bajo modalidad 8X5XNBD, a partir de las 8:00 a.m.
- **iii.** Atención en sitio: Soporte en sitio en horario hábil bajo modalidad 8X5XNBD, a partir de las 8:00 a.m.
- **iv.** Registro de número de incidentes ante partner y fabrica: Para cualquier tipo de soporte se debe generar ticket del incidente tanto del partner como de fábrica, para verificación del estado y seguimiento del mismo por parte de la Universidad Distrital Francisco José de caldas

5.2.1. Mantenimiento preventivo: Se entiende por mantenimiento preventivo, las estrategias que pretenden maximizar la vida útil y operativa de los equipos switches y sus componentes, identificando las posibles causas que pueden originar fallas futuras e indicando las medidas a tomar para evitarlas.

Durante el periodo de garantía y soporte del contrato, se debe realizar una (1) rutina de mantenimiento preventivo por año, la cual debe ser coordinada previamente con la supervisión y que incluya como mínimo:

- **a.** Backup de la configuración.
- **b.** Revisión de puertos y tarjetas.
- **c.** Backup y verificación de registros sobre eventos y/o alarmas.
- **d.** Diagnóstico de registros sobre eventos y/o alarmas.
- **e.** Apagado de acuerdo a manuales.
- **f.** Mantenimiento preventivo a hardware (físico)
- **g.** Actualización de software y firmware si aplica, en caso de presentar problemas en el desempeño se debe revertir el parche o firmware que se instaló y se debe conservar la versión que garantice el correcto funcionamiento.
- **h.** Revisiones generales.
- **i.** Puesta en correcto funcionamiento y verificación de servicios.

5.2.2. Mantenimiento correctivo: Se entiende por mantenimiento correctivo, todas las actividades y procedimientos que conlleve a la solución de las fallas que se presenten en la infraestructura descrita en el presente documento, como también la solución de estas y la puesta en operación normal del equipo y sus componentes.

El mantenimiento correctivo puede derivar de un mantenimiento preventivo en el que se evidencia una falla o de una falla detectada y reportada por el equipo técnico de la Red de Datos de la Universidad Distrital.

El contratista puede realizar el diagnóstico de la falla de manera remota, de no ser posible, debe enviar un ingeniero al sitio donde se encuentra ubicado el equipo en falla en un plazo menor o igual a veinticuatro (24) horas para corregir el inconveniente o verificar la necesidad de reemplazo de la parte. (RMA).

El Tiempo máximo para remplazo de equipos, tarjetas y partes, será de un (1) día hábil después de diagnosticada la falla.

Los elementos que se requieran reemplazar deben ser nuevos, originales y ensamblados de fábrica. Adicionalmente el equipo nuevo deberá tener características iguales o superiores al equipo que fue diagnosticado para reemplazar mediante RMA.

5.2.3. Documentación soporte de actividades de mantenimiento

- **a.** El contratista debe entregar documento con el esquema de escalamiento SLA para niveles de servicio.
- **b.** Entrega en medio digital de los registros de eventos y fallas.
- **c.** Reporte de visita técnica: Se debe generar siempre que el contratista realice una visita en sitio y debe incluir como mínimo: serial del equipo, fecha, soporte y datos de contacto, líneas telefónicas, correos electrónicos, procedimientos realizados, observaciones y hallazgos.
- **d.** Informe técnico: en un plazo no mayor a cinco (5) días hábiles de realizado el mantenimiento (preventivo o correctivo), el contratista debe presentar a la supervisión del contrato el informe de las actividades realizadas, este informe debe incluir como mínimo:
  - **i.** Fecha de la actividad
  - **ii.** Equipos intervenidos con su respectivo serial
  - **iii.** Actividades realizadas
  - **iv.** Descripción, análisis y recomendaciones resultantes de la lectura del registro de eventos y fallas presentes para los mantenimientos preventivos.
  - **v.** Diagnóstico y concepto técnico sobre la falla, causas, soluciones y recomendaciones (Si aplica)
  - **vi.** Listado de seriales y denominación de partes reemplazadas y retiradas (Si aplica).

5.3. Actualización de software (update y upgrade): Las actualizaciones "*update*" son aquellas que se implementan para corregir errores, mejorar el rendimiento de los equipos o implementar nuevas funciones o características sin cambiar la versión principal del software, mientras que las "*upgrade*" implican una mejora o cambio sustancial, como la instalación de una versión más reciente con nuevas funciones o mejoras significativas.

El contratista, previo a la ejecución de una actualización, debe informar al correo designado por la supervisión el tipo de actualización a realizar, las actividades a ejecutar, el tiempo estimado que tomará la actualización y si esta causa afectación de los servicios prestados. La Unidad Red de Datos confirmará por correo electrónico la ejecución de la actualización.

Para todas las actualizaciones se deben tener en cuenta las siguientes actividades:

- **a.** Backup de la configuración.
- **b.** Revisión de puertos y tarjetas.
- **c.** Backup y verificación de registros sobre eventos y/o alarmas.
- **d.** Diagnóstico de registros sobre eventos y/o alarmas.
- **e.** Apagado de acuerdo a manuales.
- **f.** Actualización de software, en caso de presentar problemas en el desempeño se debe revertir las actualizaciones de software que se instaló y se debe conservar la versión que garantice el correcto funcionamiento.
- **g.** Revisiones generales.
- **h.** Puesta en correcto funcionamiento y verificación de servicios.

6. Pruebas

El contratista deberá realizar pruebas iniciales de recepción, encendido, arranque e identificación sobre la totalidad de los equipos suministrados, incluyendo switches, access points, fuentes de poder, módulos, transceptores y demás componentes asociados, con el fin de verificar que los equipos se encuentran en correcto estado físico y operativo antes de cualquier actividad de configuración o integración con la infraestructura tecnológica de la Universidad Distrital Francisco José de Caldas.

Las pruebas tendrán como propósito validar que cada equipo encienda correctamente, complete su secuencia de arranque sin errores críticos, sea reconocido por el sistema operativo o plataforma correspondiente, y que la información lógica del equipo coincida con la información física registrada en etiquetas, empaques o documentación del fabricante.

Para cada equipo, el contratista deberá generar un archivo individual en formato digital, preferiblemente .txt, .log o .pdf, en el cual se evidencie como mínimo la siguiente información:

- **a.** Tipo de equipo.
- **b.** Marca.
- **c.** Modelo y Referencia
- **d.** Número de serie físico.
- **e.** Número de serie lógico reportado por el equipo.
- **f.** Versión de sistema operativo, firmware o imagen instalada.
- **g.** Secuencia completa de arranque del equipo.
- **h.** Estado general posterior al arranque.
- **i.** Inventario de hardware reconocido por el equipo.
- **j.** Estado de fuentes de poder, ventiladores, módulos, interfaces y transceptores, cuando aplique.
- **k.** Evidencia de ausencia de alarmas o errores críticos durante el arranque.
- **l.** Fecha de ejecución de la prueba.

El contratista deberá entregar, además del archivo individual de evidencia por cada equipo suministrado, un documento general consolidado de pruebas iniciales, en el cual se relacione la totalidad de los equipos verificados y se resuman los resultados de las pruebas de inspección física, encendido, secuencia de arranque, identificación, inventario básico de hardware, versión de software o firmware, estado inicial de componentes y ausencia de alarmas críticas.

El documento consolidado deberá ser entregado en formato digital y PDF, y deberá estar firmado por el responsable técnico del contratista que elaboró las pruebas y por el supervisor del contrato o delegado técnico designado por la Universidad, dejando constancia de la revisión y aceptación inicial de los equipos o de las observaciones que correspondan.

La Universidad podrá solicitar la repetición de las pruebas, aclaraciones técnicas o reemplazo de equipos cuando se presenten inconsistencias entre la información física y lógica del equipo, fallas de encendido, errores durante la secuencia de arranque, alarmas críticas, fallos de hardware, ausencia de reconocimiento de componentes o cualquier condición que impida validar satisfactoriamente el estado inicial del equipo.

7. Glosario

- **8x5xNBD**: Servicio de soporte disponible 5 días hábiles de la semana de 8:00 am a 5:00 pm, que incluye atención de incidentes y, de ser necesario, reemplazo de hardware al siguiente día hábil.
- **Actualización (Update):** Correcciones menores, parches de seguridad o mejoras funcionales aplicadas a una solución tecnológica sin implicar un cambio de versión principal.
- **Actualización mayor (Upgrade):** Cambio de versión de un sistema o software que incorpora mejoras significativas, nuevas funcionalidades o modificaciones estructurales.
- **Alta disponibilidad (HA):** Configuración tecnológica que permite mantener la operación continua de un sistema o servicio ante fallas de alguno de sus componentes, mediante mecanismos de redundancia y conmutación automática.
- **RMA:** Return Merchandise Authorization (Autorización de Devolución de Mercancía), es un proceso usado por fabricantes o proveedores para gestionar la devolución, reparación o reemplazo de equipos y/o partes defectuosas.
- **Backup:** es una copia de seguridad de datos, sistemas o archivos que se almacena para poder recuperarlos en caso de pérdida, daño, falla o ataque informático.
- **Site Survey (Mapa de calor):** Estudio técnico de cobertura inalámbrica que permite identificar intensidad de señal, interferencias y desempeño de la red Wi-Fi mediante representaciones gráficas.
- **Switch:** Dispositivo de red que interconecta equipos dentro de una red local y administra el envío de datos entre ellos de manera eficiente.
- **Access Point (AP):** Dispositivo de red que permite la conexión inalámbrica de equipos a una red local mediante tecnología Wi-Fi.
- **NAC (Network Access Control):** Solución de seguridad que controla y valida el acceso de usuarios y dispositivos a la red según políticas definidas.
- **SLA (Service Level Agreement):** Acuerdo de nivel de servicio que define métricas, tiempos de respuesta, disponibilidad y responsabilidades entre proveedor y cliente.
- **MU-MIMO (Multi-User Multiple Input Multiple Output):** Tecnología Wi-Fi que permite transmitir datos simultáneamente a múltiples dispositivos para mejorar el rendimiento de la red.
- **Spatial Streams:** Flujos de datos independientes transmitidos de manera simultánea en redes inalámbricas para aumentar velocidad y capacidad de transmisión.

- **Beamforming:** Tecnología de optimización Wi-Fi que dirige la señal inalámbrica hacia dispositivos específicos para mejorar cobertura y estabilidad.
- **BeamFlex:** Tecnología de antenas inteligentes desarrollada por Ruckus Networks que ajusta dinámicamente los patrones de señal para optimizar cobertura y rendimiento inalámbrico.
- **Omnidireccional:** Tipo de antena que transmite y recibe señal en múltiples direcciones alrededor de su eje.
- **SDN (Software-Defined Networking):** Arquitectura de red que centraliza y automatiza la administración de la infraestructura mediante software.
- **Ransomware:** Tipo de malware que cifra o bloquea información y exige un pago para restaurar el acceso a los datos.
- **DDoS (Distributed Denial of Service):** Ataque informático que sobrecarga un servicio o red mediante múltiples conexiones simultáneas para interrumpir su operación.
- **RFC (Request for Comments):** Documento técnico que define estándares, protocolos y buenas prácticas relacionadas con tecnologías de Internet y redes.
- **Jumbo Frame**: Trama de red Ethernet con tamaño superior al estándar tradicional, utilizada para mejorar eficiencia en transmisión de datos.
- **Memoria DRAM**: Memoria volátil utilizada para almacenamiento temporal de datos en ejecución dentro de equipos y dispositivos electrónicos.
- **Memoria Flash:** Memoria no volátil que permite almacenar información de forma permanente en dispositivos electrónicos y de almacenamiento.
- **PoE (Power over Ethernet):** Tecnología que permite transmitir energía eléctrica y datos a través de un mismo cable de red Ethernet para alimentar dispositivos como Access Points, cámaras IP y teléfonos VoIP.