ESPECIFICACIONES TÉCNICAS

RENOVACIÓN (ADQUISICIÓN) DE EQUIPOS DE COMUNICACIÓN LAN y WLAN

1. AREA USUARIA

Departamento de Informática.

2. FINALIDAD PÚBLICA

La ejecución de este proyecto tiene como finalidad brindar una infraestructura tecnológica óptima para el buen desempeño de las áreas administrativas y educativas, en cumplimiento de los fines institucionales del SENCICO.

3. ACTIVIDAD DEL POI

Modernizar la Gestión Institucional de SENCICO.

4. OBJETO DE LA CONVOCATORIA

Se requiere seleccionar a una persona jurídica para la adquisición de un Equipo de Comunicaciones LAN para las sedes de SENCICO.

Objetivos específicos:

- Adquirir equipos de comunicaciones, para renovar los equipos actuales con el que cuenta SENCICO, para el uso eficiente del servicio de Internet y otros servicios del área administrativa y educativa del SENCICO.
- Mantener la operatividad y continuidad de los servicios que brinda SENCICO, soportados en equipos e infraestructura de última generación.

5. SISTEMA DE CONTRATACIÓN

Suma Alzada.

6. MODALIDAD DE EJECUCIÓN

Llave en mano.

7. CARACTERÍSTICAS TÉCNICAS

ITEM	Prestación	Descripción	Cantidad	Unidad de Medida
I	Principal	Entrega de equipos de comunicaciones LAN y WLAN	01	Global
		Implementación de equipos de comunicaciones LAN y WLAN	01	Unidad
	Accesoria	Soporte Técnico	01	Servicio
		Mantenimiento	01	Servicio
		Capacitación	01	Servicio

CONSIDERACIONES GENERALES:

- El Contratista se encargará de la instalación, configuración y puesta en marcha de los equipos de comunicaciones.
- El Contratista deberá retirar los equipos de comunicaciones actuales (equipo a reemplazar) del gabinete correspondiente, el mismo que deberá ser previa coordinación con el personal del Departamento de Informática.
- Se deberá considerar lo necesario para que la instalación, configuración y puesta en marcha de los equipos de comunicaciones, se realice sin afectar los servicios que actualmente se vienen ejecutando sobre la infraestructura actual.
- El Contratista deberá realizar un backup de actual equipo e implementará y configurará los nuevos equipos con las funciones similares de acuerdo a las características de los servicios que brinda el equipo en su actual ubicación.

- Los bienes adquiridos deberán ser de primer uso, y año de fabricación como mínimo 2020.
- Dentro del Plazo de Entrega, se deberá ejecutar un protocolo de pruebas, el cual no deberá contar con observaciones para dar la conformidad respectiva.
- El postor presentará en un Anexo al momento de la presentación de la oferta, donde liste la relación de los números de parte o código, marca, modelo de los bienes propuestos, adjuntando información técnica como folletos, catálogos o brochure o similares de los bienes que está ofertando, emitidas por el fabricante; que pueden ser presentados en idioma español o traducidos de manera oficial, esto debido a que dicha documentación es ESCENCIAL para la revisión del cumplimiento de la oferta (equipos ofrecidos versus equipos requeridos). Y en caso los documentos antes mencionados no precisen alguna característica solicitada en el presente requerimiento, se aceptará una Carta de fabricante indicando el cumplimiento correspondiente.
- SENCICO autorizará el ingreso a las instalaciones al personal del CONTRATISTA previa solicitud detallada, donde deberán presentar: datos del personal, N° de DNI, materiales a ingresar de ser el caso, fechas y horarios de ingreso, Declaración Jurada mencionada en el ítem 7.5.8 del "PLAN PARA LA VIGILANCIA, PREVENCIÓN Y CONTROL DEL COVID-19 EN EL SENCICO", pruebas serológicas con vigencia de 30 días calendarios, como mínimo 48 horas hábiles antes del permiso solicitado, por correo electrónico.
- El personal del CONTRATISTA deberá utilizar en forma obligatoria la mascarilla desde su ingreso hasta su salida, dicha mascarilla deberá cubrir la boca y la nariz firmemente que no haya espacio de separación con la cara, así mismo los guantes de látex serán de uso obligatorio.
- El CONTRATISTA deberá considerar los equipos y herramientas necesarias para llevar a cabo la correcta instalación e implementación del Bien.
- El personal que lleve a cabo las actividades de instalación de los Equipos de comunicaciones, deberá contar con el Equipo de protección Personal adecuado y de Bioseguridad, de acuerdo a las tareas a realizar.
- De existir algún accidente será responsabilidad del Contratista.
- EL CONTRATISTA deberá realizar todas las configuraciones básicas, intermedias y avanzada de redes (networking), de acuerdo las indicaciones dadas por el Departamento de Informática.
- EL CONTRATISTA deberá habilitar las configuraciones de seguridad de los Switch para accesos a la administración de los mismos en remoto y por consola, seguridad en los puertos, del CIS (Center for Internet Security), configuración de vlans y protocolos GVRP, intervlan routing, prioridades y listas de acceso necesarias.
- El CONTRATISTA deberá considerar los componentes, aplicaciones, suscripciones, licenciamiento, etc. necesarias para llevar a cabo la correcta implementación y configuración de los equipos de comunicaciones.
- En caso los equipos requieran licenciamiento de funcionamiento o modalidad de suscripción, dado que no son perpetuos, se deberá considerar para los todos los equipos ofertados mínimo 5 años de habilitación de todas las funcionalidades, con el fin de garantizar el funcionamiento de los equipos y evitar interrupciones en el servicio en caso de vencimiento de garantía y soporte.
- El modelo del equipo ofertado no deberá entrar en obsolescencia tecnológica (fin de venta – EoL) dentro de los siguientes 03 años. Se precisa que se podrá sustentar lo solicitado con una carta de fabricante donde se indique que los equipos ofertados no tienen anuncio de fin de venta; y que de anunciarse en los próximos 03 años la fecha fin de venta (EoL), los equipos ofertados mantendrán soporte vigente como mínimo los siguientes próximos 05 años.
  Este documento deberá presentarse a la presentación de ofertas.
  Se aceptará también una carta de fabricante indicando que los modelos de los equipos ofertados pertenecen a la última generación de equipos lanzados al mercado y que no se encuentran en obsolescencia tecnológica o con fecha anunciada de fin de venta (EOS).

- El fabricante de los Equipos Switches debe estar presente en los últimos 4 reportes de Gartner en el cuadrante de Líderes para Wired and Wireless LAN Access de los años 2016, 2017, 2018 y 2019; para lo cual a la presentación de la oferta deberá presentar estos 04 últimos reportes.
- Se precisa que SENCICO cuenta con cableado UTP Categoría 6A y fibra óptica Multimodo LC/LC. Por lo que, el Contratista deberá considerar lo necesario para la conexión de los equipos a instalar al actual cableado estructurado de la Entidad.

CARACTERISTICAS TECNICAS:

A. TIPO 1: Switch de 24 puertos – No POE – Uso de Acceso

Características físicas del Switch

- Formato 1UR
- El Switch debe contar con veinticuatro (24) puertos ethernet de 1Gbps
- El switch debe contar con cuatro (4) puertos uplink SFP/SFP+ o superior.
- Incluir al menos, 02 transceivers multimodo sfp+ LC SR 300m por switch.
- Un Puerto USB (USB-A o USB 2.0).
- Administración por Consola RJ-45 o USB-C.
- fuentes de alimentación fijas o modulares.

Capacidades del Hardware

- Almacenamiento interno (flash) mínimo 4 GB
- Memoria interna (sd-ram o dram) mínimo 4 GB.
- Tamaño del búfer de al menos 8 MB.
- Velocidad o tasa de reenvío mínima 95 Mpps.
- Capacidad de Conmutación mínima 128 Gbps.

Alta disponibilidad

- En capa 2 deberá contar con tecnología de stack o apilamiento que permita que el switch se pueda conectar a otro equipo de la misma familia y formar una única unidad lógica (switch lógico) que permita la agregación de puertos usando dos puertos conectados a dos switches diferentes. La cantidad mínima de switches por stack soportados deberá ser de 8 (ocho).
- Los equipos deben soportar mínimo 40 Gbps de velocidad de stack.
- LACP (link aggregation control protocol)

Características mejoradas del Sistema Operativo

- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red.
- Debe permitir la configuración de puertos SPAN (Switched Port Analyzer) o port mirroring para funciones de monitoreo y análisis.
- El equipo debe permitir su operación en modo tradicional y en modo SDN (redes definidas por software o en modo que permita automatizar y segmentar la red en modo dinámico) sin necesidad de adquirir ningún componente de hardware adicional (módulos o tarjetas) o licenciamiento en el mismo switch (de requerirlo incluir las licencias necesarias).
- Debe proporcionar visibilidad granular y proveer de monitoreo de la red en tiempo muy cercano a tiempo real (se admite sFlow como sustento).
- El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback.
- La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El motor de analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST u otro. Debe tener Base de datos para guardar configuración, datos de estados operativos y analítica. Este

servicio debe estar habilitado e incluido de manera perpetua o por lo menos 5 años. Este motor de analítica debe ser capaz de al menos presentar y monitorear información de salud de los equipos y alertar en caso de alguna falla. El motor de analítica deberá considerar un esquema que asegure la alta disponibilidad de sus funciones.

- Debe contar con mecanismos para implementación automática al contar con una conexión al NMS o internet, sin intervención de servicio técnico especializado.
- Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
- Capacidad mediante el switch o software adicional de despliegue controlado de configuración y administración con su proceso de auditoría y control de cambios, chequeo de consistencia de configuración y compliance.
- Los protocolos de enrutamiento dinámicos deberán estar habilitados para toda la capacidad que tiene el hardware
- **Se deben ofertar todas las funcionalidades habilitadas del switch por el tiempo de vida útil del equipo o como mínimo por 5 años.**

Características en Capa 2

- Debe soportar por lo menos 4094 Vlans IDs.
- Encapsulación de VLAN IEEE 802.1Q.
- VLAN troncalizadas.
- Rapid Per-VLAN STP Plus ó IEEE 802.1w.
- MSTP (IEEE 802.1s).
- Spanning Tree port edge o port fast.
- Spanning Tree para protección del port root.
- Spanning Tree para protección del Bridge root o un equivalente para evitar la propagación de Notificaciones de Cambio de Topologia TCN
- LACP (IEEE 802.3ad).
- Control de tormentas en unicast, multicast, broadcast y mutlicast.
- Encapsulado para virtualización de red VXLAN (habilitado).
- Número de direcciones MAC 16,000.

Multicast

- Protocolo de Gestión de Grupo de Internet (IGMP) versión 2 y 3.
- IGMP Snooping.
- MLD v1 y v2.

Capacidades de Calidad de Servicio

- Clase de Servicio CoS Capa 2 IEEE 802.1p.
- Strict Priority (SP), Deficit Weighted Round (DWRR) o Shaped Round Robin (SRR).

Métodos de Seguridad del equipo

- ACLs de entrada estándar y extendida sobre ethernet.
- Acls habilitado para IPv4, IPv6.
- Incluir módulo TPM (Trusted Platform Module) o TAM (Trust Anchor Module) o también modulo o chip para asegurar la autenticidad del hardware y del código del equipo.
- Servicio de autenticación remota (RADIUS).
- Dispositivo debe manejar control de acceso via TACACs+ para AAA (autenticación, autorización y accounting) para definir los accesos de usuarios administradores por privilegios.

Funciones de administración en el equipo

- SSHv2
- Telnet opcional
- AAA
- RADIUS
- Syslog

- SNMP v1, v2 o v2c y v3
- Monitoreo remoto (RMON)
- Usuarios y claves unificados a través de CLI y SSH.
- Network Time Protocol (NTP)
- Pruebas de diagnóstico durante el arranque
- Netflow, SFlow o similar.

Estándares

- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1p: CoS Prioritization
- IEEE 802.1Q: VLAN Tagging
- IEEE 802.1s: Multiple VLAN Instances of Spanning Tree Protocol
- IEEE 802.1w: Rapid Reconfiguration of Spanning Tree Protocol
- IEEE 802.3z: Gigabit Ethernet
- IEEE 802.3ad: Link Aggregation Control Protocol (LACP)
- IEEE 802.3ae: 10 Gigabit Ethernet
- IEEE 802.1ab: LLDP

B. TIPO 3: Switch de 24 puertos – POE – Uso de Acceso

Características físicas del Switch

- Formato 1UR
- El Switch debe contar con veinticuatro (24) puertos ethernet de 1Gbps PoE+ 370w.
- PoE Budget 370 watts como mínimo.
- El switch debe contar con cuatro (4) puertos uplink SFP/SFP+ o superior.
- Incluir al menos, 02 transceivers multimodo sfp+ LC SR 300m por switch.
- Un (1) Puerto USB (USB-A o USB 2.0).
- Administración por Consola RJ-45 o USB-C.
- fuentes de alimentación fijas o modulares.

Capacidades del Hardware

- Almacenamiento interno (flash) mínimo 4GB
- Memoria interna (sd-ram o dram) mínimo 4GB.
- Tamaño del búfer de al menos 8 MB.
- Velocidad o tasa de reenvío mínima 95 Mpps.
- Capacidad de Conmutación mínima 128 Gbps.

Alta disponibilidad

- En capa 2 deberá contar con tecnología de stack o apilamiento que permita que el switch se pueda conectar a otro equipo de la misma familia y formar una única unidad lógica (switch lógico) que permita la agregación de puertos usando dos puertos conectados a dos switches diferentes. La cantidad mínima de switches por stack soportados deberá ser de 8 (ocho).
- Los equipos deben soportar mínimo 40 Gbps de velocidad de stack.
- LACP (link aggregation control protocol)

Características mejoradas del Sistema Operativo

- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red.
- Debe permitir la configuración de puertos SPAN (Switched Port Analyzer) o port mirroring para funciones de monitoreo y análisis.
- El equipo debe permitir su operación en modo tradicional y en modo SDN (redes definidas por software o en modo que permita automatizar y segmentar la red en modo dinámico) sin necesidad de adquirir ningún componente de hardware adicional (módulos o tarjetas) o licenciamiento en el mismo switch (de requerirlo incluir las licencias necesarias).

- Debe proporcionar visibilidad granular y proveer de monitoreo de la red en tiempo muy cercano a tiempo real (se admite sFlow como sustento).
- El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback.
- La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El motor de analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST u otro. Debe tener Base de datos para guardar configuración, datos de estados operativos y analítica. Este servicio debe estar habilitado e incluido de manera perpetua o por lo menos 5 años. Este motor de analítica debe ser capaz de al menos presentar y monitorear información de salud de los equipos y alertar en caso de alguna falla. El motor de analítica deberá considerar un esquema que asegure la alta disponibilidad de sus funciones.
- Debe contar con mecanismos para implementación automática al contar con una conexión al NMS o internet, sin intervención de servicio técnico especializado.
- Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
- Capacidad mediante el switch o software adicional de despliegue controlado de configuración y administración con su proceso de auditoría y control de cambios, chequeo de consistencia de configuración y compliance.
- Los protocolos de enrutamiento dinámicos deberán estar habilitados para toda la capacidad que tiene el hardware
- **Se deben ofertar todas las funcionalidades habilitadas del switch por el tiempo de vida útil del equipo o como mínimo por 5 años.**

Características en Capa 2

- Debe soportar por lo menos 4094 Vlans IDs.
- Encapsulación de VLAN IEEE 802.1Q.
- VLAN troncalizadas.
- Rapid Per-VLAN STP Plus ó IEEE 802.1w.
- MSTP (IEEE 802.1s).
- Spanning Tree port edge o port fast.
- Spanning Tree para protección del port root.
- Spanning Tree para protección del Bridge root o un equivalente para evitar la propagación de Notificaciones de Cambio de Topologia TCN
- LACP (IEEE 802.3ad).
- Control de tormentas en unicast, multicast, broadcast y mutlicast.
- Encapsulado para virtualización de red VXLAN (habilitado).
- Número de direcciones MAC 16,000.

Multicast

- Protocolo de Gestión de Grupo de Internet (IGMP) versión 2 y 3.
- IGMP Snooping.
- MLD v1 y v2.

Capacidades de Calidad de Servicio

- Clase de Servicio CoS Capa 2 IEEE 802.1p.
- Strict Priority (SP), Deficit Weighted Round (DWRR) o Shaped Round Robin (SRR).

Métodos de Seguridad del equipo

- ACLs de entrada estándar y extendida sobre ethernet.
- Acls habilitado para IPv4, IPv6.
- Incluir módulo TPM (Trusted Platform Module) o TAM (Trust Anchor Module) o también modulo o chip para asegurar la autenticidad del hardware y del código del equipo.
- Servicio de autenticación remota (RADIUS).

- Dispositivo debe manejar control de acceso via TACACs+ para AAA (autenticación, autorización y accounting) para definir los accesos de usuarios administradores por privilegios.

Funciones de administración en el equipo

- SSHv2
- Telnet opcional
- AAA
- RADIUS
- Syslog
- SNMP v1, v2 o v2c y v3
- Monitoreo remoto (RMON)
- Usuarios y claves unificados a través de CLI y SSH.
- Network Time Protocol (NTP)
- Pruebas de diagnóstico durante el arranque
- Netflow, SFlow o similar.

Estándares

- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1p: CoS Prioritization
- IEEE 802.1Q: VLAN Tagging
- IEEE 802.1s: Multiple VLAN Instances of Spanning Tree Protocol
- IEEE 802.1w: Rapid Reconfiguration of Spanning Tree Protocol
- IEEE 802.3z: Gigabit Ethernet
- IEEE 802.3ad: Link Aggregation Control Protocol (LACP)
- IEEE 802.3ae: 10 Gigabit Ethernet
- IEEE 802.1ab: LLDP

C. TIPO 5: Switch de 48 puertos –POE – Uso de Acceso

Características físicas del Switch

- Formato 1UR
- El Switch debe contar con cuarenta y ocho (48) puertos ethernet de 1Gbps PoE+ 740w.
- PoE Budget 740 watts como mínimo.
- El switch debe contar con cuatro (4) puertos uplink SFP/SFP+ o superior.
- Incluir al menos, 02 transceivers multimodo sfp+ LC SR 300m por switch.
- Un (1) Puerto USB (USB-A o USB 2.0).
- Administración por Consola RJ-45 o USB-C.
- fuentes de alimentación fijas o modulares.

Capacidades del Hardware

- Almacenamiento interno (flash) mínimo 4GB
- Memoria interna (sd-ram o dram) mínimo 4GB.
- Tamaño del búfer de al menos 8 MB.
- Velocidad o tasa de reenvío mínima 130 Mpps.
- Capacidad de Conmutación mínima 176 Gbps.

Alta disponibilidad

- En capa 2 deberá contar con tecnología de stack o apilamiento que permita que el switch se pueda conectar a otro equipo de la misma familia y formar una única unidad lógica (switch lógico) que permita la agregación de puertos usando dos puertos conectados a dos switches diferentes. La cantidad mínima de switches por stack soportados deberá ser de 8 (ocho).
- Los equipos deben soportar mínimo 40 Gbps de velocidad de stack.
- LACP (link aggregation control protocol)

Características mejoradas del Sistema Operativo

- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red.
- Debe permitir la configuración de puertos SPAN (Switched Port Analyzer) o port mirroring para funciones de monitoreo y análisis.
- El equipo debe permitir su operación en modo tradicional y en modo SDN (redes definidas por software o en modo que permita automatizar y segmentar la red en modo dinámico) sin necesidad de adquirir ningún componente de hardware adicional (módulos o tarjetas) o licenciamiento en el mismo switch (de requerirlo incluir las licencias necesarias).
- Debe proporcionar visibilidad granular y proveer de monitoreo de la red en tiempo muy cercano a tiempo real (se admite sFlow como sustento).
- El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback.
- La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El motor de analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso Apis del tipo REST u otro. Debe tener Base de datos para guardar configuración, datos de estados operativos y analítica. Este servicio debe estar habilitado e incluido de manera perpetua o por lo menos 5 años. Este motor de analítica debe ser capaz de al menos presentar y monitorear información de salud de los equipos y alertar en caso de alguna falla. El motor de analítica deberá considerar un esquema que asegure la alta disponibilidad de sus funciones.
- Debe contar con mecanismos para implementación automática al contar con una conexión al NMS o internet, sin intervención de servicio técnico especializado.
- Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
- Capacidad mediante el switch o software adicional de despliegue controlado de configuración y administración con su proceso de auditoría y control de cambios, chequeo de consistencia de configuración y compliance.
- Los protocolos de enrutamiento dinámicos deberán estar habilitados para toda la capacidad que tiene el hardware
- **Se deben ofertar todas las funcionalidades del switch habilitadas por el tiempo de vida útil del equipo o al menos por 5 años**.

Características en Capa 2

- Debe soportar por lo menos 4094 Vlans IDs.
- Encapsulación de VLAN IEEE 802.1Q.
- VLAN troncalizadas.
- Rapid Per-VLAN STP Plus ó IEEE 802.1w.
- MSTP (IEEE 802.1s).
- Spanning Tree port edge o port fast.
- Spanning Tree para protección del port root.
- Spanning Tree para protección del Bridge root o un equivalente para evitar la propagación de Notificaciones de Cambio de Topologia TCN
- LACP (IEEE 802.3ad).
- Control de tormentas en unicast, multicast, broadcast y mutlicast.
- Encapsulado para virtualización de red VXLAN (habilitado).
- Número de direcciones MAC 16,000.

Multicast

- Protocolo de Gestión de Grupo de Internet (IGMP) versión 2 y 3.
- IGMP Snooping.
- MLD v1 y v2.

Capacidades de Calidad de Servicio

- Clase de Servicio CoS Capa 2 IEEE 802.1p.
- Strict Priority (SP), Deficit Weighted Round (DWRR) o Shaped Round Robin (SRR).

Métodos de Seguridad del equipo
- ACLs de entrada estándar y extendida sobre ethernet.
- Acls habilitado para IPv4,IPv6.
- Incluir módulo TPM (Trusted Platform Module) o TAM (Trsut Anchor Module) o también modulo o chip para asegurar la autenticidad del hardware y del código del equipo.
- Servicio de autenticación remota (RADIUS).
- Dispositivo debe manejar control de acceso via TACACs+ para AAA (autenticación, autorización y accounting) para definir los accesos de usuarios administradores por privilegios.

Funciones de administración en el equipo
- SSHv2
- Telnet opcional
- AAA
- RADIUS
- Syslog
- SNMP v1, v2 o v2c y v3
- Monitoreo remoto (RMON)
- Usuarios y claves unificados a través de CLI y SSH.
- Network Time Protocol (NTP)
- Pruebas de diagnóstico durante el arranque
- Netflow, SFlow o similar.

Estándares
- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1p: CoS Prioritization
- IEEE 802.1Q: VLAN Tagging
- IEEE 802.1s: Multiple VLAN Instances of Spanning Tree Protocol
- IEEE 802.1w: Rapid Reconfiguration of Spanning Tree Protocol
- IEEE 802.3z: Gigabit Ethernet
- IEEE 802.3ad: Link Aggregation Control Protocol (LACP)
- IEEE 802.3ae: 10 Gigabit Ethernet
- IEEE 802.1ab: LLDP

D. TIPO 4: Switch de 48 puertos –No POE – Uso de Acceso

Características físicas del Switch
- Formato 1UR
- El Switch debe contar con cuarenta y ocho (48) puertos ethernet de 1Gbps.
- El switch debe contar con cuatro (4) puertos uplink SFP/SFP+ o superior.
- Incluir al menos, 02 transceivers multimodo sfp+ LC SR 300m por switch.
- Un (1) Puerto USB (USB-A o USB 2.0).
- Administración por Consola RJ-45 o USB-C.
- fuentes de alimentación fijas o modulares.

Capacidades del Hardware
- Almacenamiento interno (flash) mínimo 4GB
- Memoria interna (sd-ram o dram) total mínimo 4GB.
- Tamaño del búfer de al menos 8 MB.
- Velocidad o tasa de reenvío mínima 130 Mpps.
- Capacidad de Conmutación mínima 176 Gbps.

Alta disponibilidad
- En capa 2 deberá contar con tecnología de stack o apilamiento que permita que el switch se pueda conectar a otro equipo de la misma familia y formar una única unidad

lógica (switch lógico) que permita la agregación de puertos usando dos puertos conectados a dos switches diferentes. La cantidad mínima de switches por stack soportados deberá ser de 8 (ocho).
- Los equipos deben soportar mínimo 40 Gbps de velocidad de stack.
- LACP (link aggregation control protocol)

Características mejoradas del Sistema Operativo
- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red.
- Debe permitir la configuración de puertos SPAN (Switched Port Analyzer) o port mirroring para funciones de monitoreo y análisis.
- El equipo debe permitir su operación en modo tradicional y en modo SDN (redes definidas por software o en modo que permita automatizar y segmentar la red en modo dinámico) sin necesidad de adquirir ningún componente de hardware adicional (módulos o tarjetas) o licenciamiento en el mismo switch (de requerirlo incluir las licencias necesarias).
- Debe proporcionar visibilidad granular y proveer de monitoreo de la red en tiempo muy cercano a tiempo real (se admite sFlow como sustento).
- El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback.
- La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El motor de analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST u otro. Debe tener Base de datos para guardar configuración, datos de estados operativos y analítica. Este servicio debe estar habilitado e incluido de manera perpetua o por lo menos 5 años. Este motor de analítica debe ser capaz de al menos presentar y monitorear información de salud de los equipos y alertar en caso de alguna falla. El motor de analítica deberá considerar un esquema que asegure la alta disponibilidad de sus funciones.
- Debe contar con mecanismos para implementación automática al contar con una conexión al NMS o internet, sin intervención de servicio técnico especializado.
- Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
- Capacidad mediante el switch o software adicional de despliegue controlado de configuración y administración con su proceso de auditoría y control de cambios, chequeo de consistencia de configuración y compliance.
- Los protocolos de enrutamiento dinámicos deberán estar habilitados para toda la capacidad que tiene el hardware
- **Se deben ofertar todas las funcionalidades del switch habilitadas por el tiempo de vida útil del equipo o al menos por 5 años.**

Características en Capa 2
- Debe soportar por lo menos 4094 Vlans IDs.
- Encapsulación de VLAN IEEE 802.1Q.
- VLAN troncalizadas.
- Rapid Per-VLAN STP Plus ó IEEE 802.1w.
- MSTP (IEEE 802.1s).
- Spanning Tree port edge o port fast.
- Spanning Tree para protección del port root.
- Spanning Tree para protección del Bridge root o un equivalente para evitar la propagación de Notificaciones de Cambio de Topologia TCN
- LACP (IEEE 802.3ad).
- Control de tormentas en unicast, multicast, broadcast y mutlicast.
- Encapsulado para virtualización de red VXLAN (habilitado).
- Número de direcciones MAC 16,000.

Multicast
- Protocolo de Gestión de Grupo de Internet (IGMP) versión 2 y 3.
- IGMP Snooping.
- MLD v1 y v2.

Capacidades de Calidad de Servicio
- Clase de Servicio CoS Capa 2 IEEE 802.1p.
- Strict Priority (SP), Deficit Weighted Round (DWRR) o Shaped Round Robin (SRR).

Métodos de Seguridad del equipo
- ACLs de entrada estándar y extendida sobre ethernet.
- Acls habilitado para IPv4,IPv6.
- Incluir módulo TPM (Trusted Platform Module) o TAM (Trust Anchor Module) o también modulo o chip para asegurar la autenticidad del hardware y del código del equipo.
- Servicio de autenticación remota (RADIUS).
- Dispositivo debe manejar control de acceso via TACACs+ para AAA (autenticación, autorización y accounting) para definir los accesos de usuarios administradores por privilegios.

Funciones de administración en el equipo
- SSHv2
- Telnet opcional
- AAA
- RADIUS
- Syslog
- SNMP v1, v2 o v2c y v3
- Monitoreo remoto (RMON)
- Usuarios y claves unificados a través de CLI y SSH.
- Network Time Protocol (NTP)
- Pruebas de diagnóstico durante el arranque
- Netflow, SFlow o similar.

Estándares
- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1p: CoS Prioritization
- IEEE 802.1Q: VLAN Tagging
- IEEE 802.1s: Multiple VLAN Instances of Spanning Tree Protocol
- IEEE 802.1w: Rapid Reconfiguration of Spanning Tree Protocol
- IEEE 802.3z: Gigabit Ethernet
- IEEE 802.3ad: Link Aggregation Control Protocol (LACP)
- IEEE 802.3ae: 10 Gigabit Ethernet
- IEEE 802.1ab: LLDP

E. TIPO 6: Switch de 48 puertos –POE – Uso de Core

Características físicas del Switch
- Formato 1UR
- El Switch debe contar con cuarenta y ocho (48) puertos ethernet de 1Gbps Full PoE+ (1440w).
- El switch debe contar con cuatro (4) puertos uplink
- Mínimo 2 puertos de 40 Gbps o 4 puertos tipo sfp28 o superior.
- Un (1) Puerto USB (micro USB o USB 2.0).
- Administración por Consola RJ-45 o USB-C.
- Cantidad de fuentes de alimentación redundantes 2.
- Bandeja de ventiladores, redundantes o en spare.

Capacidades del Hardware

- Almacenamiento interno de al menos 16GB
- Memoria interna total de 8GB.
- Tamaño del búfer de al menos 8 MB.
- Velocidad o tasa de reenvío mínima 351 Mpps.
- Conmutación Capa 2 y Capa 3 mínima (sin incluir modulo externo de stack) 472 Gbps.

Alta disponibilidad

- En capa 2 deberá contar con tecnología de stack o apilamiento que permita que el switch se pueda conectar a otro equipo de la misma familia y formar una única unidad lógica (switch lógico) que permita la agregación de puertos usando dos puertos conectados a dos switches diferentes. La cantidad mínima de switches por stack soportados deberá ser de 8 (ocho)
- Los equipos deben soportar hasta 200 Gbps de velocidad de stack.
- En capa 3 deberá contar con enrutamiento estático y protocolos de enrutamiento dinámico como: BGP, OSPF y opcionalmente RIP.
- Las unidades de fuente de alimentación son intercambiables en caliente.
- Debe incluirse todas las fuentes y ventiladores disponibles (con redundancia de componentes internos o componetes en spare).
- Mecanismos de alta disponibilidad incluidas (VRRP).

Características mejoradas del Sistema Operativo

- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red.
- Debe permitir la configuración de puertos SPAN (Switched Port Analyzer) o port mirroring para funciones de monitoreo y análisis.
- Compatibilidad completa de protocolos de enrutamiento unicast y multicast de Capa 3 para BGP, OSPF, PIM-SM (RFC 4601), y opcionalmente RIPv2) y MSDP (RFC 3618).
- El equipo debe permitir su operación en modo tradicional y en modo SDN (redes definidas por software o en modo que permita automatizar y segmentar la red en modo dinámico) sin necesidad de adquirir ningún componente de hardware adicional (módulos o tarjetas) o licenciamiento en el mismo switch (de requerirlo incluir las licencias necesarias).
- Debe proporcionar visibilidad granular y proveer de monitoreo de la red en tiempo muy cercano a tiempo real (se admite sFlow como sustento).
- El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback.
- La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST u otro. Debe tener Base de datos para guardar configuración, datos de estados operativos y analítica. Este servicio debe estar habilitado e incluido de manera perpetua o por lo menos 5 años. Este motor de analítica debe ser capaz de al menos presentar y monitorear información de salud de los equipos y alertar en caso de alguna falla. El motor de analítica deberá considerar un esquema que asegure la alta disponibilidad de sus funciones.
- Debe contar con mecanismos para implementación automática al contar con una conexión al NMS o internet, sin intervención de servicio técnico especializado.
- Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
- Capacidad mediante el switch o software adicional de despliegue controlado de configuración y administración con su proceso de auditoría y control de cambios, chequeo de consistencia de configuración y compliance.
- Los protocolos de enrutamiento dinámicos deberán estar habilitados para toda la capacidad que tiene el hardware
- Las funcionalidades que se buscan para los switches deberán estar habilitadas por toda la vida útil.

- **Se deben ofertar todas las funcionalidades habilitadas del switch por el tiempo de vida útil del equipo o al menos por 5 años**.

Características en Capa 2
- Debe soportar por lo menos 4090 Vlans.
- Encapsulación de VLAN IEEE 802.1Q.
- VLAN troncalizadas.
- Rapid Per-VLAN STP Plus ó IEEE 802.1w.
- MSTP (IEEE 802.1s).
- Spanning Tree port edge o port fast.
- Spanning Tree para protección del port root.
- Spanning Tree para protección del Bridge root o un equivalente para evitar la propagación de Notificaciones de Cambio de Topologia TCN
- LACP (IEEE 802.3ad).
- Control de tormentas en unicast, multicast, broadcast y mutlicast.
- Encapsulado para virtualización de red VXLAN (habilitado)
- Número de direcciones MAC 32,000.

Características en Capa 3
- Interfaces L3 Routed Ports ó Interfaces Virtuales de Switch (SVIs). Al menos 1000.
- Routing ECMP de al menos 4 rutas que permita evitar cuellos de botella incrementando la resiliencia y aumentando la capacidad con mínima disrupción en la red.
- Debe soportar entradas de ACL en Capa 3 y Capa 4.
- Capacidad de la tabla de ruteo de al menos 32,000 entradas de host unicast.
- Routing IPv6: Static, OSPFv3.
- Routing IPv4: Static, OSPF y opcionalmente RIPv2.
- Protocolos de Redundancia de Router Virtual VRRP.
- Debe soportar la tecnología VXLAN habilitada

Multicast
- Multicast: PIM, PIM-SM.
- Protocolo de Gestión de Grupo de Internet (IGMP) versión 2 y 3.

Capacidades de Calidad de Servicio
- Clase de Servicio CoS Capa 2 IEEE 802.1p.
- 8 colas de hardware por puerto.
- Configuración de QoS por puerto.
- CoS trust.
- Asignación de CoS por puerto.
- CLI para la implementación QoS.
- Clasificación de QoS basado en ACL en Capa 2, 3 y 4.
- Marcado de Clase de Servicio por CLI.
- Marcado de DSCP Differentiated services Code Point.
- Encolamiento de salida basado en CoS.
- Enrutamiento basado en políticas.

Métodos de Seguridad del equipo
- ACLs de entrada estándar y extendida sobre ethernet.
- ACLs Capa 3 y 4 estándar y extendida para IPv4, ICMP, TCP y UDP.
- ACLs basado en VLAN ó que las ACLs se basen en VLAN, segmentos de red o rangos de IPs
- ACLs basado en puertos.
- DHCP snooping con Option 82
- DHCP Server
- DHCP relay.
- ARP dinámica Address Resolution Protocol.
- Configuración de Políticas de Plano de Control.

Funciones de administración en el equipo
- SSHv2
- Telnet opcional
- AAA
- RADIUS
- Syslog
- SNMP v1, v2 o v2c y v3
- Soporte XML u otro lenguaje de programación.
- Monitoreo remoto (RMON)
- Usuarios y claves unificados a través de CLI y SSH.
- RBAC
- Network Time Protocol (NTP)
- Pruebas de diagnóstico durante el arranque
- Netflow, SFlow o similar.

Estándares
- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1p: CoS Prioritization
- IEEE 802.1Q: VLAN Tagging
- IEEE 802.1s: Multiple VLAN Instances of Spanning Tree Protocol
- IEEE 802.1w: Rapid Reconfiguration of Spanning Tree Protocol
- IEEE 802.3z: Gigabit Ethernet
- IEEE 802.3ad: Link Aggregation Control Protocol (LACP)
- IEEE 802.3ae: 10 Gigabit Ethernet
- IEEE 802.1ab: LLDP

F. TIPO 7: Switch de Core Tipo Chassis

Características físicas del Switch
- Switch modular
- Incluir al menos 4 bahías para módulos I/O
- L2, L3, L4
- Fuentes de poder redundantes
- Soporte interfaces 1G /10G / 25G / 40G / 100G
- El equipo debe incluir al menos dos (2) bahías para módulos de administración.
- Los módulos de administración deben operar al menos en modo activo/pasivo.
- La solución debe incluir al menos 02 módulos de administración por switch Core.

Capacidades del Hardware
- Incluir al menos las capacidades en las tarjetas modulares:
  - ✓ 96 interfaces RJ45 1000Base-T
  - ✓ 08 interfaces 10G SFP+ de fibra óptica
  - ✓ 24 interfaces 1G SFP de fibra óptica
- Cada interface de fibra óptica debe incluir su transceivers del tipo LC SR multimodo
- Todos los interfaces incluidos deben ser no bloqueantes.
- Una vez incluidos los interfaces solicitados, el equipo ofertado debe contar con al menos 01 bahía libre para crecimiento futuro.
- Cada bahía I/O debe soportar como mínimo un BW de conexión de 2.4 Tbps
- RAM: 16 GB.
- Flash: 32 GB (puede ser cubierto por memoria externa).
- El sistema operativo debe incluir la última versión completa (con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar) liberada por el fabricante a la fecha de la compra.
- Debe traer todos los accesorios para montaje y operación en rack estándar de 19".
- Máximo 8 RUs (unidades de rack).

- El equipo debe soportar de fuentes de poder redundante internas, con característica de instalación en caliente (hot-swap). Redundancia N+1 o N+N
- Incluir:
  - ✓ Fuentes de poder AC.
  - ✓ El Equipo debe venir con todas las fuentes de poder disponibles.

Administración y Monitoreo
- un (1) interfaz consola serial RJ45, USB-C o mini USB
- un (1) interfaz Ethernet para administración fuera de banda.
- un (1) puerto USB-A.

Acceso y configuración
- Línea serial de comandos (CLI)
- Telnet (opcional)
- Web
- SSH v2
- REST API u otro
- Debe contar con mecanismos para implementación automática al contar con una conexión al NMS o internet, sin intervención de servicio técnico especializado.
- Soporte de múltiples configuraciones almacenadas en la memoria flash. Capacidad de crear y almacenar de manera manual y automática la configuración a modo de checkpoints de modo que se pueda regresar de manera sencilla a una configuración anterior.
- SNMP v1, v2c, v3
- RMON
- sFlow (RFC 3176) o netflow.
- IPv6 host
- IPv6 Dual Stack
- Soporte de port mirroring local

Stacking
Capacidad de conectarse en stack con otro equipo igual ofreciendo las siguientes características:
- La tecnología de stacking debe estar basada en Multi Chassis LAG (MC-LAG)
- Deben ser percibidos por los demás equipos como un único switch de modo que se pueda configurar agregación de puertos entre ellos.
- No deben compartir los servicios relacionados al plano de control, enrutamiento y gestión de modo que se pueda garantizar alta disponibilidad ante la falla de un chasis y la actualización de software.
- La configuración debe poder sincronizarse entre los miembros del stack
- Los miembros del stack deben operar en modo activo-activo tanto en L2 como en L3.
- Incluir todo el hardware que requiera la conexión del stack para:
  - ✓ Al menos dos (2) enlaces de 100Gbps entre los equipos.
  - ✓ Longitud de los cables al menos de tres (3) metros o más.

Características mejoradas del Sistema Operativo
- El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback.
- La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST u otro. Debe tener Base de datos para guardar configuración, datos de estados operativos y analítica. Este servicio debe estar habilitado e incluido de manera perpetua o por lo menos 5 años. Este motor de analítica debe ser capaz de al menos presentar y monitorear información de salud de los equipos y alertar en caso de alguna falla. El motor de analítica deberá considerar un esquema que asegure la alta disponibilidad de sus funciones.

- Debe contar con mecanismos para implementación automática al contar con una conexión al NMS o internet, sin intervención de servicio técnico especializado.
- Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
- **Todas las funcionalidades habilitadas por el tiempo de vida útil del equipo o al menos por 5 años.**
- Capacidad mediante el switch o software adicional de despliegue controlado de configuración y administración con su proceso de auditoría y control de cambios, chequeo de consistencia de configuración y compliance.

Características en Capa 2

- Mac address table de al menos 32000 direcciones MAC.
- Soporte de 4094 VLAN ID.
- MVRP o similar.
- VXLAN (habilitado)
- Soporte de tramas de 9000 bytes como mínimo.
- IEEE 802.1Q.
- IEEE 802.1w.
- IEEE 802.1p.
- IEEE 802.1X.
- IEEE 802.3ad.
- Listas de control de acceso (ACL) tanto para IPv4 e IPv6:
  - ✓ Aplicables a puertos y VLANs
  - ✓ Parámetros configurables de Capa 2 (MAC origen/destino), Capa 3 (IP/subred origen/destino) y Capa 4
- LACP IEEE 802.3ad:
  - ✓ Soporte de grupos estáticos y dinámicos.
- Soporte de:
  - ✓ MSTP
  - ✓ RPVST+ o PVRST+
  - ✓ STP Root guard
  - ✓ STP BPDU port protection

Características en Capa 3

- Protocolos enrutados en IPv4 y IPv6
- Tamaño de las tablas al menos:
  - ✓ Rutas unicast: 64000, se precisa que este parámetro es mínimo entre la sumatoria de las rutas unicast IPv4 e IPv6.
  - ✓ Rutas multicast: 7500
  - ✓ Tamaño de la tabla host (ARP): 32000
- Protocolos para IPv4 al menos:
  - ✓ Enrutamiento: estático.
  - ✓ Enrutamiento Inter-Vlan.
  - ✓ OSPF
  - ✓ BGP
- Protocolos para IPv6 al menos:
  - ✓ Enrutamiento: estático.
  - ✓ OSPF
  - ✓ BGP
- Manejo de rutas al menos:
  - ✓ Equal-Cost Multipath para rutas estáticas habilita multiples enlaces de igual costo para incrementar la redundancia y escalabilidad.
- IPv4/IPv6 multicast al menos:
  - ✓ IGMP v2/v3 (Internet Group Management Protocol)
  - ✓ MLD v1/v2

- ✓ PIM SM
- DHCP: Soporte para asignar direccionamiento IP dinámico mediante protocolo DHCP en IPv4 e IPv6
- Otras funcionalidades
  - ✓ VRRP
  - ✓ VRF (mínimo 64)
  - ✓ Policy Base Routing

QoS
Soporte de:

- ✓ DSCP local-priority mapping
- ✓ Strict priority (SP) u otro
- ✓ DWRR u otro
- ✓ QOS trust COS
- ✓ QOS trust DSCP

Seguridad

- Autenticación por dirección MAC
- RADIUS
- TACACS+. Dispositivo debe manejar control de acceso via TACACs+ para AAA (autenticación, autorización y accounting) para definir los accesos de usuarios administradores por privilegios.
- Capacidad de configurar políticas en el plano de control de modo que se pueda limitar los flujos por protocolos hacia el CPU impidiendo ataques DOS.
- IGMP y MLD snooping
- DHCP Snooping
- UDLD

G. SOLUCION DE GESTIÓN Y CONTROL DE ACCESO

La Solución de Gestión y Control de Acceso; deben soportar Ipv4 e Ipv6 y deben proveer las siguientes funcionalidades:

SOLUCIÓN DE GESTIÓN

- Puede estar compuesto por una o más plataformas/software de la misma marca de los switches, access points y controladoras inalámbricas.
- Puede ser en formato appliance o en servicio cloud.
- En el caso de los Access Point los cuales sean gestionados en nube, este deberá estar habilitado en licenciamiento o equivalente, como mínimo por 5 años, de tal manera no dejen de funcionar o brindar conectividad wifi, evitando interrupciones a las estaciones cliente.
- En caso los equipos requieran licenciamiento de funcionamiento o modalidad de suscripción, dado que no son perpetuos, se deberá considerar para los todos los equipos ofertados mínimo 5 años de habilitación de todas las funcionalidades, con el fin de garantizar el funcionamiento de los equipos y evitar interrupciones en el servicio en caso de vencimiento de garantía y soporte.
- El licenciamiento deberá garantizar el total monitoreo de los dispositivos, como los Puntos de Acceso (AP), controladores inalámbricos, equipos gestionados de la solución de comunicaciones unificadas propuesta y el total de Switches ofertados. Los switches actuales podrán ser monitoreados con al menos las funcionalidades básicas por medio de SNMP.
- Operatividad con el protocolo SNMP v2 (ó 2c) y v3, SSH, APIs u otros para la gestión de la red.
- Capacidad de administrar de forma centralizadas y personalizada a todo los Switches, a través de conexiones seguras.
- Capacidad de gestión y aplicación de políticas de calidad de servicio (QoS) de forma centralizada y personalizada a todos los Switches.
- Capacidad de graficar el mapa de topología de la red para identificar el estatus (conectado o desconectado) de los Switches, APs y controladores.

- Capacidad de gestión y aplicación de políticas de control de tráfico (ACL) de forma centralizada y personalizada a todos los Switches.
- Capacidad de enviar alertas (vía correo, a varios destinos) ante:
  - ✓ Caídas (apagados) de puertos de los Switches.
  - ✓ Temperatura mayor a un valor umbral
  - ✓ Consumo de CPU mayor a un valor umbral
  - ✓ Consumo de memoria mayor a un valor umbral
- La solución debe incluir la funcionalidad de visualización de tráfico en tiempo real de los equipos Switches, controlador y APs ofertados.
- Visualización y analítica de tráfico que permita reducir los tiempos de resolución de incidencias en los equipos ofertados.
- La solución deberá ser multi-vendor, sobre todo garantizando los switches que tiene en la actualidad la entidad, con las funcionalidades básicas de monitoreo por SNMP.
- Cabe indicar que la solución es del tipo llave en mano, el postor deberá de proveer de todos los elementos necesarios para el funcionamiento de la solución.

SOLUCIÓN DE SEGURIDAD Y CONTROL DE ACCESO

- El software deber permitir la Seguridad y Control de Acceso para todos los equipos ofertados y todos los equipos que actualmente cuenta la Entidad.
- La solución debe incluir gestión de políticas, analíticas y atomización en la aplicación de directivas de accesos.
- Deberá tener licenciamiento perpetuo. De no contar con ellos deberá proveer 2 años adicionales a la cantidad de años por garantía/soporte.
- Deberá soportar la aplicación de políticas de control de acceso para redes de cualquier tipo (LAN, WLAN y VPN) sobre los distintos fabricantes de equipos de acceso Enterprise que existan en el mercado
- La solución debe centralizar el control de acceso de usuarios administradores a dispositivos de red de la entidad vía TACACS.
- La solución debe basarse en un esquema AAA (autenticación, autorización y accounting).
- Debe ser capaz de actuar como Autoridad Certificadora (CA–Certificate Authority).
- Se deberá de considerar la implementación o costo de certificados digitales de ser necesarios.
- Interface basada en WEB para la configuración de políticas y troubleshooting.
- El sistema deberá contar con funcionalidad habilitada para proporcionar integración con las siguientes fuentes de autenticación externas existentes: Directorio Activo de Windows, integración con Mobile Device Management (MDM), servidores RADIUS y RADIUS token server, entre otros.
- Deberá soportar Auto Sign-On y/o single sign-on (SSO) mediante SAML
- Deberá soportar reconocimiento de diversos dispositivos presentes en la red, permitiendo automatizar el aprovisionamiento de los dispositivos y controlar el acceso a la red mediante certificado digital.
- Deberá permitir autenticación 802.1x, no 802.1x y acceso basado en portal web.
- Soporte de varias fuentes de autenticación Tales como RADIUS, LDAP, AD, HTTP, SQLy Okta.
- Los tipos de enforcements aplicados para cada uno de los servicios de autenticación deben ser como mínimo:
  - ✓ RADIUS enforcement permit / deny / CoA
  - ✓ Policy assignment
  - ✓ DACL
  - ✓ TACACS+
  - ✓ Filter Id
- El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multi dominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario.
- La solución debe soportar y tener habilitados los siguientes métodos de autenticación como mínimo:

- ✓ PAP
- ✓ CHAP
- ✓ EAP-MSCHAPv2
- ✓ EAP-MD5
- ✓ PEAP
- ✓ EAP-TLS
- ✓ Machine Authentication
- ✓ Autenticación GTC contra un Token Server que actúe como RADIUS server.
- ✓ EAP-FAST

- La solución debe, dependiendo del perfil del usuario autenticado, poder asignarle políticas de manera granular de acuerdo a las siguientes condiciones combinadas o independientes:
  - ✓ Acceso a la red basado en tiempos: Determinación de intervalos de tiempo en donde está permitido el usuario en la red.
  - ✓ Acceso de red basado en la localización del usuario en la red: En determinados lugares de la red permitir el acceso del usuario.
  - ✓ Acceso de red basado en el tipo de acceso: Ante determinados medios de acceso como WLAN, VPN, LAN. si está autorizado darle acceso a la red.
  - ✓ Atributos extraídos del directorio activo o personalizaciones vía API.
- De acuerdo a las condiciones descritas, poder aplicar algún tipo de política al usuario. Como mínimo las siguientes:
  - ✓ Asignación dinámica de vlans
  - ✓ Asignación dinámica de listas de control de acceso.
  - ✓ Redirección hacia una URL.
- Deberá permitir utilizar atributos de múltiples repositorios de identidad tales como Microsoft Active Directory, LDAP, base de datos SQL compatibles con ODBC, servidores de Token y base de datos interna, con el objetivo de utilizar estos atributos dentro de una política para un control granular.

Reconocimiento de dispositivos (profiling)

- Descubrir y clasificar los dispositivos finales, independientemente del tipo de dispositivo. Por ejemplo: Impresora, dispositivo móvil, computadora, teléfono, entre otros.
- Identificación y clasificación (profiling) basada en datos contextuales tales como:
  - ✓ MAC OUIs
  - ✓ Nmap Scan
  - ✓ DHCP fingerprints
  - ✓ TCP fingerprints
  - ✓ HTTP user agent
  - ✓ SNMP traps
  - ✓ LLDP
- La funcionalidad de profiling debe estar licenciada para el 100% de conexiones simultáneas, debe ser capaz de identificar cambios en perfilamiento y modificar dinámicamente la autorización de privilegios. Es decir, si una impresora que ya había sido autenticada en el pasado aparece como una Laptop Windows, el sistema de control de acceso debe denegar el acceso de manera automática.
- Debe permitir al administrador sobrescribir la clasificación de perfilamiento hecha por el sistema, o agregar una nueva regla de clasificación para los atributos aprendidos, a modo de permitir que endpoints desconocidos sean categorizados de manera adecuada.

Administración de acceso para dispositivos headless

- Deberá permitir identificar a los dispositivos no administrados no 802.1x (headless) – impresoras, teléfonos y cámaras IP y clasificarlos como conocido o desconocido.
- Esta funcionalidad deberá estar disponible y habilitada para su despliegue.

Gestión de visitantes

- Deberá permitir crear perfiles de accesos la creación de cuentas temporales de invitados para el acceso a la red WIFI y cableada.

- Deberá permitir la creación de más de un portal cautivo para la gestión de visitas.
- El portal cautivo incluirá funcionalidades avanzadas de auto-registro, mediante las cuales el invitado podrá generar su propia cuenta de invitado sin comprometer la seguridad de la red.
- El portal proporcionará diversos métodos para la entrega de credenciales de invitado: email, SMS o impresión de tickets.
- El portal proporcionará métodos avanzados de aprobación de la visita por parte de la persona que recibe al invitado que permitan autorizar la visita de manera flexible y sin intervención de personal de IT.
- Identificación de usuarios recurrentes para bloqueo de mal uso de la gestión de visitas.
- Se valorarán las posibilidades de personalización del portal de invitados como:
  - ✓ Inclusión en el portal de menús desplegables que permitan registrar información relativa al invitado (motivo de la visita, duración de la misma, persona a la que visita, etc.
  - ✓ Generación de portales HTML de distinto en función del tamaño y resolución de las pantallas de los dispositivos móviles.
  - ✓ Posibilidad de incluir todo tipo de contenido multimedia en el portal: imágenes, audio y/o video.

Plataforma

- Plataforma con capacidad para al menos 2500 conexiones simultáneas cada nodo.
- Licenciamiento de autenticación mínimo: 2500 conexiones simultáneas sobre las cuales se debe incorporar para el 100% de dispositivos las funcionalidades descritas en características generales, reconocimiento de dispositivos, administración de acceso para dispositivos headless y gestión de visitantes

Repositorios de identidad soportados

- Deberá soportar Microsoft Active Directory
- Deberá soportar LDAP
- Deberá soportar SQL server compatible con ODBC
- Deberá soportar base de datos internas.

H. PUNTO DE ACCESO INALAMBRICO PARA INTERIORES

Características:

- Equipo de punto de acceso de red inalámbrica (AP) de diseño para interiores.
- El equipo debe ser totalmente nuevo de fábrica cuyo modelo no entre en obsolescencia tecnológica (fin de venta – EoS) dentro de los siguientes 03 años.
- Arquitectura con y sin controlador
- El equipo debe soportar mínimo:
  - ✓ Doble radio.
  - ✓ MU-MIMO 4x4:4ss en la radio de 5Ghz.
  - ✓ Hasta 5.3 Gbps desempeño
  - ✓ Al menos 16 SSID.
  - ✓ Asignación y selección de canal de manera automática y niveles de potencia del equipo.
  - ✓ Soporte hasta de 512 clientes asociados por radio
  - ✓ DFS
  - ✓ MRC
  - ✓ CSD
  - ✓ OFDMA
  - ✓ TWT
- Deben soportar al menos los siguientes estándares de la industria:
  - ✓ IEEE 802.11a
  - ✓ IEEE 802.11b
  - ✓ IEEE 802.11g
  - ✓ IEEE 802.11n
  - ✓ IEEE 802.11ac

- ✓ IEEE 802.11ax
- ✓ Wi-FI Alliance Certified

- Ancho de canal:
  - ✓ 802.11n high-throughput (HT) support: HT20/40
  - ✓ 802.11ac very high throughput (VHT) support: VHT20/40/80/160
  - ✓ 802.11ax high efficiency (HE) support: HE20/40/80/160
- El equipo debe soportar al menos las siguientes velocidades: 4800Mbps en 5ghz y 574 Mbps en 2.4 Ghz.
- Radios
  - ✓ 2,4Ghz
  - ✓ 5,0Ghz
  - ✓ Bluetooth
  - ✓ Zigbee (con capacidad a futuro)
- Interface minimo un puerto 10/100/1000BASE-T Ethernet y un puerto 100/1000/2500BASE T o un puerto 100/1000/2500/5000BASE-T
- Seguridad WPA, WPA2 y WPA3 – Enterprise 192-bit mode, Enhanced Open (OWE)
- Antenas internas con una ganancia de 4dBi en el radio de 2,4Ghz y 6dBi en el radio de 5Ghz
- Equipo debe ser Wi-Fi 6 certificado por la WiFi Alliance.
- Rango de temperatura en operación de 0° C a +50° C
- Rango de humedad en operación de 10% a 90% sin condensación.
- Alimentación Eléctrica de 802.3af/at/bt

I. PUNTO DE ACCESO INALAMBRICO PARA EXTERIORES

- Equipo de punto de acceso de red inalámbrica (AP) de diseño para exteriores.
- El equipo debe ser totalmente nuevo de fábrica cuyo modelo no entre en obsolescencia tecnológica (fin de venta – EoS) dentro de los siguientes 03 años.
- El equipo debe soportar mínimo:
  - ✓ Doble radio.
  - ✓ MIMO 4x4:3ss en la radio de 5Ghz.
  - ✓ Hasta 1.3 Gbps desempeño
  - ✓ Al menos 16 SSID.
  - ✓ Asignación y selección de canal de manera automática y niveles de potencia del equipo.
  - ✓ Soporte hasta de 256 clientes asociados por radio
  - ✓ DFS
  - ✓ MRC
  - ✓ CSD
- Deben soportar al menos los siguientes estándares de la industria:
  - ✓ IEEE 802.11a
  - ✓ IEEE 802.11b
  - ✓ IEEE 802.11g
  - ✓ IEEE 802.11n
  - ✓ IEEE 802.11ac
  - ✓ Wi-FI Alliance Certified
- Ancho de canal
  - ✓ 802.11n high-throughput (HT) support: HT20/40
  - ✓ 802.11ac very high throughput (VHT) support: VHT20/40/80
- Soporte ambiental IP67
- Radios
  - ✓ 2,4Ghz
  - ✓ 5,0Ghz
- Interface minumo un puerto 10/100/1000BASE-T Ethernet
- Seguridad WPA, WPA2 y WPA3 (opcional)
- Antenas Internas
- Equipo debe ser Wi-Fi 6 certificado por la WiFi Alliance.
- Rango de temperatura en operación de -40° C a +55° C
- Rango de humedad en operación de 5% a 90% sin condensación
- Alimentación Eléctrica de 802.3af o at

J. EQUIPO CONTROLADOR

Dos (02) equipos controladores de última generación que cumpla como mínimo las siguientes características:

- Los equipos deben ser totalmente nuevo de fábrica cuyo modelo no entre en obsolescencia tecnológica (fin de venta – EoS) dentro de los siguientes 03 años.
- Los dos equipos controladores deberán estar implementados en alta disponibilidad y debe incluir todo el licenciamiento, accesorios, partes, complementos, configuraciones que se requieran para operar en dicha modalidad.
- El controlador debe soportar al menos 250 APs, a través de la actualización de licencias.
- La solución ofertada debe incluir las licencias para controlar los APs ofertados.
- El controlador debe soportar APs de tipo indoors (interiores) y outdoor (exteriores)
- Soporte mínimo de 8,000 dispositivos clientes, concurrentemente.
- Número mínimo de interfaces: 2 puertos SFP+
- Debe manejar los estándares 802.11 a/b/g/n/ac/ax.
- Debe ser capaz de controlar y administrar los puntos de acceso inalámbrico de forma centralizada incluyendo las funciones de actualización de configuraciones y software.
- En el evento de una falla en el controlador, los puntos de acceso inalámbrico deberán poder encontrar de forma automática un controlador de respaldo.
- Deberá de contar con software que le permita adaptarse y administrar en tiempo real el entorno de RF. Entre estas funciones deberá de encontrarse:
  - ✓ Asignación dinámica de canales para optimizar la cobertura y desempeño.
  - ✓ Balanceo de carga de usuarios entre múltiples puntos de acceso inalámbricos.
  - ✓ Detección y corrección de huecos en la cobertura inalámbrica.
  - ✓ Control dinámico de potencia de acuerdo a las condiciones de la red.
  - ✓ En caso de falla de un punto de acceso inalámbrico, el controlador deberá de ser capaz de ajustar la potencia en los puntos de acceso adyacentes para cubrir el área que fue afectada.
  - ✓ Detección y capacidad de evitar interferencia 802.11 mediante la re calibración de la red.
  - ✓ Deberá soportar mecanismos de detección y mitigación de interferencia no 802.11n en tiempo real dentro del canal como fuera del canal de atención gracias al uso de puntos de acceso soportados para tal funcionalidad. Como mínimo debe de realizar lo siguiente:
    - Detección basada en la causa de la interferencia.
    - Capacidad de poder cambiar de canal inalámbrico ante saturación y/o interferencias, así como incrementar o reducir la potencia de las antenas ante eventos en el RF.
    - Clasificación de la interferencia, entre ellas hornos microondas, teléfonos analógicos inalámbricos, cámaras de video, dispositivos bluetooth, etc.
- Detección y clasificación de puntos de acceso inalámbricos no legítimos de manera automática, con opción a llevar acciones de contención como alguna de las siguientes:
  - ✓ Contención en el aire. Los puntos de acceso de la solución permiten contener al rogue incrementando su señal u otro mecanismo similar para que el cliente se asocie a la red adecuada.
  - ✓ Contención en la red. Integración con la plataforma de switches que permita identificar con la información de la red inalámbrica el punto de red a la cual se ha conectado el rogue. Debe de poder inclusive, realizar un apagado de puerto o bloquear el tráfico del AP no autorizado.
  - ✓ Enviar paquetes de interferencia al dispositivo ilegítimo para desconectarlo de la red inalámbrica.
- Debe de soportar y tener habilitado mecanismos de protección de los mensajes de administración entre cliente-punto de acceso y punto de acceso-controlador. Por lo menos debe de asegurar la encriptación de los mensajes de administración desde los clientes.
- Seguridad en capa 2 mediante el manejo de filtrado por MAC, WEP, WEP dinámico, TKIP, WPA, 802.11i (WPA2), WPA3. WPA3-Enterprise, 802.1X (PEAP, EAP-TLS, EAP-TTLS) y L2TP o IPSEC.
- Capacidad de poder manejar autenticaciones basadas en web que pueda servir para la autenticación de usuarios invitados.

- Bloqueo de tráfico entre clientes asociados a un mismo SSID.
- Soporte de AAA mediante un servidor de RADIUS/TACACS+ para manejar las políticas de usuarios y derechos de gestión del equipo.
- Deberá de soportar y tener habilitado autenticación de usuarios en base a un servidor de RADIUS, base de datos local, base de datos LDAP, directorio activo de Microsoft, entre otros.
- Debe incluir o estar integrado a una solución DPI (Deep Packet Inspection o similar) con la cual se pueda visualizar, analizar y controlar el uso de tráfico a nivel capa 7 (aplicación).
- Debe incluir un firewall statefull L3, L4 y L7 embebido. De no soportarlo se deberá proporcionar un firewall externo a la solución.
- Debe poder identificar las aplicaciones que usan los clientes con la finalidad de permitir o restringir su uso además de establecer la velocidad de carga y descarga de cada una (shaping).
- Permitir o denegar el uso de aplicaciones
- Deberá de ofrecer servicios de roaming entre puntos de acceso inalámbrico, sin importar que estos se encuentren en diferente subred y sin hacer cambios en la infraestructura de LAN, preservando las características del acceso en términos de QoS y Seguridad y logrando que el delay sea imperceptible por las aplicaciones de misión crítica como es el caso de la voz.
- Deberá soportar y tener habilitada las siguientes funcionalidades de calidad de servicio:
  - ✓ Soporte de Wi-Fi Multimedia
  - ✓ Manejo de 802.1p
  - ✓ Soporte de DSCP
  - ✓ Soporte de 802.11e
- Soporte de asignación de ancho de banda por perfil de usuario de acuerdo a su rol en la red y en el directorio activo
- Soporte y habilitado de IGMP para la optimización del tráfico multicast.
- Debe tener la capacidad de funcionar como servidor de DHCP o DHCP Proxy o DHCP Relay.
- Soporte de IPv4 e IPv6.
- Para la administración como mínimo debe de soportar el acceso via HTTP, HTTPS, Telnet, SSH, SNMP v2c, v3.
- Debe manejar los estándares 802.11 d/e/h.
- Debe de tener la capacidad de poder identificar los dispositivos que se conectan a la red y poder crear reglas basado en su identidad.
- Debe estar integrado con sistemas WIPS/WIDS o tener uno embebido en el mismo equipo, con el cual se puede lograr como mínimo lo siguiente:
  - ✓ Permitir ejecutar un trazado dentro de la red cableada para la ubicación de los posibles AP rogue conectados a la red. En caso de hacerlo a través de una integración con WIPS se debe incluir la solución completa de software, hardware y licenciamiento que permita esta funcionalidad.
  - ✓ El sistema debe contar con mecanismos precisos y automáticos para la clasificación real de Access Points intrusos que se encuentren en la red.
  - ✓ La solución debe proveer mecanismos automáticos y eficientes de contención de Access Points intrusos.
  - ✓ La detección de ataques avanzados, habilitar acciones de contención o mitigación de amenazas avanzadas y colección de datos del WLAN.

CANTIDAD DE EQUIPOS

a) Equipos LAN

N°	CODIGO PATRIMONIAL DEL EQUIPO A REEMPLAZAR	SEDE	TIPO DE SWITCH	CANT.
1	49650	GERENCIA ZONAL AREQUIPA	TIPO 6: Switch de 48 puertos –POE – Uso de Core	01
2	49692	GERENCIA ZONAL AREQUIPA	TIPO 6: Switch de 48 puertos –POE – Uso de Core	01
3	49742	GERENCIA ZONAL CHICLAYO	TIPO 6: Switch de 48 puertos –POE – Uso de Core	01

4	49797	GERENCIA ZONAL CUSCO	TIPO 6: Switch de 48 puertos –POE – Uso de Core	01
5	49850	CENTRO DE FORMACION LOS OLIVOS	TIPO 6: Switch de 48 puertos –POE – Uso de Core	01
6	39739	CENTRO DE FORMACION SAN BORJA	TIPO 4: Switch de 48 puertos –No POE – Uso de Acceso	01
7	49911	GERENCIA ZONAL PIURA	TIPO 6: Switch de 48 puertos –POE – Uso de Core	01
8	49975	GERENCIA ZONAL TRUJILLO	TIPO 6: Switch de 48 puertos –POE – Uso de Core	01
9	42050	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
10	42045	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
11	61539	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
12	66835	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
13	42051	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
14	42049	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
15	42057	SEDE CENTRAL	TIPO 1: Switch de 24 puertos – No POE – Uso de Acceso	01
16	59951	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
17	42056	SEDE CENTRAL	TIPO 1: Switch de 24 puertos – No POE – Uso de Acceso	01
18	42060	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
19	49978	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
20	42070	SEDE CENTRAL	TIPO 7: Switch de Core Tipo Chassis	01
21	42055	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
22	42069	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
23	22446	SEDE CENTRAL	TIPO 1: Switch de 24 puertos – No POE – Uso de Acceso	01
24	42054	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
25	42061	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
26	49349	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
27	42063	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
28	42064	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
29	49747	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
30	42046	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
31	42067	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
32	42066	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
33	42068	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
34	42052	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
35	42065	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
36	42059	SEDE CENTRAL	TIPO 1: Switch de 24 puertos – No POE – Uso de Acceso	01
37	42047	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
38	61538	SEDE CENTRAL	TIPO 5: Switch de 48 puertos –POE – Uso de Acceso	01
39	42053	SEDE CENTRAL	TIPO 3: Switch de 24 puertos – POE – Uso de Acceso	01
N°	**CODIGO PATRIMONIAL DEL EQUIPO A REEMPLAZAR**	**SEDE**	**TIPO DE EQUIPO DE COMUNICACIONES**	**CANT.**
01	NA	SEDE CENTRAL	SOLUCION DE GESTIÓN Y CONTROL DE ACCESO	01

b) Equipos Wireless LAN

N°	CODIGO PATRIMONIAL DEL EQUIPO A REEMPLAZAR	SEDE	TIPO DE ACCESS POINT	CANT.
01	41874	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
02	41878	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
03	41879	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
04	41889	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
05	41883	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
06	41876	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
07	41882	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
08	50752	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
09	50765	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
10	50768	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
11	50769	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
12	41884	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
13	41881	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
14	50764	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
15	50767	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
16	50751	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
17	41887	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
18	41877	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
19	41880	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
20	41888	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
21	41886	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
22	41885	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
23	41875	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA EXTERIORES	01
24	28147	SEDE CENTRAL	PUNTO DE ACCESO INALAMBRICO PARA INTERIORES	01
N°	**CODIGO PATRIMONIAL DEL EQUIPO A REEMPLAZAR**	**SEDE**	**TIPO DE EQUIPO DE COMUNICACIONES**	**CANT.**
01	NA	SEDE CENTRAL	EQUIPO CONTROLADOR	02

8. PLAN DE TRABAJO

8.1 Plan de Trabajo de Equipos de comunicaciones LAN

El plan de trabajo deberá entregarse a los diez (10) días calendarios en formato digital, por mesa de partes virtual del SENCICO, contabilizados a partir del día siguiente de suscrito el contrato. Y deberá contener lo siguiente:

- El cronograma general de actividades (formato Project).
- Diseño de la red a implementar, que deberá incluir:
  - Topología (formato Visio).
  - Nomenclatura de rotulación de los equipos, gabinetes (formato Excel).
  - Port mapping (formato Excel).
  - Layout de gabinetes, de cómo se instalará cada equipo y componentes (formato Visio).
- Equipo de trabajo, indicando funciones y responsabilidades.
- Protocolo de Pruebas.
- Procedimientos de seguridad.
- Lista de personal con SCTR vigente.
- Declaración jurada del personal indicando lo solicitado en el punto 7.5.8 de la Resolución de Presidencia Ejecutiva N°50-2020-02.00

El Departamento de Informática, tendrá como máximo siete (07) días calendarios, una vez recepcionado el plan de trabajo, para comunicar la aceptación del plan o alguna observación al contratista.

De existir observaciones, se le comunicará al CONTRATISTA, mediante correo electrónico, dándole un plazo no menor a dos (02) días calendarios y no mayor a ocho (08) días calendarios, de acuerdo a la complejidad de las mismas.

El Contratista deberá realizar el levantamiento respectivo coordinando previamente con el Departamento de Informática, actualizando la información correspondiente, el cual deberá incluir todos los equipos de la Entidad, los que permanecerán y los que se reemplazarán, con el fin de obtener los documentos con la información actual completa.

8.2 Plan de Trabajo de mantenimiento preventivo y correctivo

El plan de trabajo deberá entregarse a los cuatrocientos veinte (420) días calendarios (en formato digital), por mesa de partes virtual del SENCICO, contabilizados desde día siguiente de la firma del Acta de Aceptación de la Infraestructura Tecnológica (Equipos de comunicaciones LAN). Y deberá contener lo siguiente:

- Planificación y cronograma general de actividades (formato Project).
- Plan de contingencia, ante falla de equipos.
- Bitácora de actividades
- Lista de equipos: Switchs y gabinete, a dar mantenimiento, indicando Modelo, marca, Número de Serie, Mac Address, dirección IP y ubicación.
- Lista de materiales, insumos y herramientas a utilizar.
- Equipo de trabajo, indicando funciones y responsabilidades.
- Formato de Protocolo de Pruebas y Formato Hoja de trabajo (checklist).
- Procedimientos de seguridad.
- Lista de personal que participara en el mantenimiento como supervisor, coordinadores, a quien escalar.
- Declaración jurada del personal indicando lo solicitado en el punto 7.5.8 de la Resolución de Presidencia Ejecutiva N°50-2020-02.00, de corresponder.

El Departamento de Informática, tendrá como máximo siete (07) días calendarios, una vez recepcionado el plan de trabajo, para comunicar la aceptación del plan o alguna observación al contratista.

De existir observaciones, se le comunicará al CONTRATISTA, mediante correo electrónico, dándole un plazo no menor a dos (02) días calendarios y no mayor a ocho (08) días calendarios, de acuerdo a la complejidad de las mismas.

9. PRESTACIONES ACCESORIAS

A. Mantenimiento Preventivo y Correctivo

Se deberá ejecutar dos (02) Mantenimientos preventivo y correctivo dentro de los 1095 (mil novecientos noventa y cinco) días calendarios, contabilizados desde día siguiente de la firma del Acta de Aceptación de la implementación de los Equipos de comunicaciones LAN y WLAN.

Consideraciones Generales**:**

a) SENCICO autorizará el ingreso a las instalaciones al personal del CONTRATISTA previa solicitud detallada, donde deberán presentar: datos del personal, N° de DNI, materiales a ingresar de ser el caso, fechas y horarios de ingreso, Declaración Jurada mencionada en el ítem 7.5.8 del “PLAN PARA LA VIGILANCIA, PREVENCIÓN Y CONTROL DEL COVID-19 EN EL SENCICO” en caso se encuentre VIGENTE, pruebas serológicas con vigencia de 30 días calendarios, previa solicitud del Departamento de Informática. Esta información deberá ser remitida a SENCICO como mínimo 48 horas hábiles antes del permiso solicitado, por correo electrónico.
b) El CONTRATISTA deberá colocar una etiqueta especificando la fecha del mantenimiento preventivo y correctivo, el N° de mantenimiento y el nombre del Contratista, en cada equipo y gabinete en donde se haya realizado el servicio, el cual deberá ser impreso. Por otro lado, las etiquetas deberán ser: adhesivas, resistente a los solventes, y de material poliéster.

c) El CONTRATISTA deberá llenar un documento “Hoja de trabajo – Checklist”, por cada equipo y gabinete a dar mantenimiento, el cual deberá estar firmado por el personal que ejecuta el mantenimiento del Contratista, el supervisor del Contratista (personal clave: especialista en redes) y el supervisor asignado por SENCICO.
d) El CONTRATISTA deberá considerar los equipos y herramientas necesarios para llevar a cabo el correcto mantenimiento del Bien, estos equipos deberán ser registrados en seguridad.
e) El personal que lleve a cabo las actividades de mantenimiento preventivo y correctivo, deberá contar con el Equipo de protección Personal adecuado a las tareas a realizar.
f) De existir algún accidente será responsabilidad del Contratista.
g) En el caso de no lograr restablecer el servicio a partir de terminado la ventana del mantenimiento, el CONTRATISTA deberá realizar las acciones necesarias con la finalidad de solucionar los problemas presentados en un lapso no mayor de cuatro (04) horas contadas a partir de reportado el problema, tales como incluir el reemplazo de un equipo y/o componente y/o accesorio (patchcords ventiladores, fuentes, etc.), temporalmente de la misma marca, con características iguales o superiores.

   Dicho remplazo temporal del equipo y/o componente y/o accesorios (patchcords ventiladores, fuentes, etc.), tendrá como tiempo máximo treinta (30) días calendarios, los cuales serán necesarios para la reparación del equipo defectuoso o en su defecto la sustitución definitiva de un equipo y/o componente y/o accesorios nuevos con características iguales o superiores al equipo defectuoso.

Las actividades a realizar serán las siguientes:

a) Para los Switches y APs:
   - Verificación de la correcta operación de los servicios que brindan los equipos, revisión y estatus de Leds, de estado de error de los equipos, así como tarjetas I/O, según corresponda.
   - Backup de la configuración del sistema, en formato digital correspondiente a la marca y modelo del Switch.
   - Revisión que todos los patch Cord (UTP) de los Switches a dar mantenimiento, tengan el rotulado de acuerdo a los estándares TIA/EIA-606A. En caso se encuentre algún patch cord sin rotulado o averiado o en condiciones deteriodadas, se deberá realizar el rotulado y/o cambio respectivo, con un patch cord categoría 6A de la marca existente.
   - Se deberá realizar el ordenamiento de los Patch Cord de los gabinetes donde se efectuarán los trabajos de mantenimiento.
   - Limpieza de equipos de comunicaciones tanto interna como externa (Tarjetas, chasis, fuente de poder y cables).
   - El contratista debe garantizar el uso de limpiadores de contactos de secado rápido apropiado para los equipos de comunicaciones, aire puro comprimido, lubricantes y pulseras antiestáticas.
   - Actualización del firmware IOS de cada uno de los equipos a la última versión estable disponible y recomendada por el fabricante.
   - Reemplazo de los componentes o accesorios defectuosos que conforman equipos; y de ser necesario deberá realizar las configuraciones del caso para restablecer los servicios correspondientes a los Switchs.
   - Al término del proceso de mantenimiento preventivo y correctivo, todos los servicios deberán de activarse en su totalidad sin dificultad, con la conformidad del Departamento de Informática a través de su Visto Bueno en el protocolo de pruebas.

B. <u>Soporte Técnico:</u>

El servicio de Soporte Técnico será brindado por el Contratista, y deberá realizarse durante un mil novecientos noventa y cinco (1095) días calendarios, contabilizados desde el día siguiente de firmado el Acta de Aceptación de la implementación de Equipos de comunicaciones LAN y WLAN, el cual debe realizarse en la modalidad de 24x7x365, y ser atendido como sigue:

Lima, se deberá contar con el SLA correspondiente:

Atención	Atención Telefónico y ON SITE	Tiempo máximo de inicio de atención	Tiempo máximo de resolución de incidencia s/cambio de equipo y/o componente	Tiempo máximo de resolución de incidencia c/cambio de equipo y/o componente y/o desplazamiento
Incidentes	24x7x365	1 hora	4 horas	24 horas

Lima - Switchs de Core (N°20 de la lista), se deberá contar con el SLA correspondiente:

Atención	Atención Telefónico y ON SITE	Tiempo máximo de inicio de atención	Tiempo máximo de resolución de incidencia s/cambio de equipo y/o componente	Tiempo máximo de resolución de incidencia c/cambio de equipo y/o componente y/o desplazamiento
Incidentes	24x7x365	1 hora	4 horas	12 horas

Provincia, se deberá contar con el SLA correspondiente:

Atención	Atención Telefónico y ON SITE	Tiempo máximo de inicio de atención	Tiempo máximo de resolución de incidencia s/cambio de equipo y/o componente	Tiempo máximo de resolución de incidencia c/cambio de equipo y/o componente y/o desplazamiento
Incidentes	24x7x365	1 hora	4 horas	48 horas

Tiempo de máximo de inicio de atención. - *Tiempo que transcurre desde el momento de reportado el incidente por parte de SENCICO (por correo y/o teléfono), hasta que el Contratista inicia la atención del mismo.*

Tiempo máximo de resolución de incidencia sin cambio de equipo y/o componente. - *Tiempo que transcurre desde que se reporta el incidente por parte de SENCICO (por correo y/o teléfono) al Contratista, hasta la solución del mismo donde no fue necesario un cambio de equipo.*

Tiempo máximo de resolución de incidencia con cambio de equipo y/o componente y/o desplazamiento de personal. - *Tiempo que transcurre desde que se reporta el incidente por parte de SENCIO (por correo y/o teléfono) al Contratista hasta la solución del mismo, donde fue necesario un cambio de equipo y/o componente (parte, pieza, accesorio, etc.)*

El contratista deberá contar con equipos y/o componentes (patch cords de cobre, ventiladores, fuentes de poder, partes, piezas etc.) provisionales, con el fin de cumplir con los SLAs correspondientes, de tal manera que la Entidad no tenga que esperar los tiempos de Reemplazo de Fabrica (RMA). Este equipo o componente provisional deberá ser de iguales o mayores características y será aprobado por el Departamento de Informática, mediante correo electrónico.

Dicho remplazo provisional tendrá como tiempo máximo treinta (30) días calendario, los cuales serán necesarios para la reparación del equipo defectuoso o en su defecto la sustitución definitiva de un equipo nuevo con características iguales o superiores al equipo defectuoso.

Los Equipos y la Entidad deberán contar con el soporte directo de fábrica con acceso a descarga de actualizaciones de sistema operativo.

El soporte deberá considerar atender cualquier tipo de incidente de los equipos de comunicaciones adquiridos, como hardware, software, aplicaciones, licencias, componentes internos, etc.

Se deberá remitir un reporte a los cinco (05) días calendario como máximo de haber cerrado el ticket de atención de manera digital por correo electrónico al personal que designe el Departamento de Informática, el cual incluirá:

- Número de Ticket.
- Incidente presentado.
- Actividades realizadas.
- Causa Raíz del incidente presentado.
- Datos y valorización (costo) del equipo de reemplazo, si es el caso.
- Nivel de escalamiento que se tuvo que realizar para solucionar el incidente.

C. CAPACITACIÓN

a) El CONTRATISTA realizará una capacitación de los equipos implementados, de un mínimo 48 horas, (24 horas para la solución de gestión y control de accesos, 08 horas para el controlador de acceso WIFI, 08 para equipos Switch y 08 para equipó WIFI), y como mínimo a 08 (ocho) personas y podrá ser realizado en forma virtual. La fecha y hora de ejecución de la capacitación se desarrollará en coordinación con **EL SENCICO,** considerando 4 horas por día como máximo en horario laboral.
b) El CONTRATISTA debe incluir y/o entregar todo el material, en digital necesario de los temas a tratar, con el propósito de aclarar suficientemente los aspectos técnicos sobre los equipos adquiridos
c) El inicio y horario de la capacitación deberá coordinarse con el Asesor en Sistemas e Informática al correo electrónico, con cinco (05) días calendario de anticipación; y se realizará como máximo dentro de los sesenta (60) días calendarios siguientes de suscrito el contrato.
d) El CONTRATISTA deberá entregar una constancia o certificado de participación a los asistentes al finalizar la capacitación, donde especifique los nombres y apellidos del personal participante, fecha y duración del curso, debiendo estar firmado por el expositor

10. RESPONSABILIDAD DEL CONTRATISTA

El Contratista es el único responsable ante SENCICO de cumplir con la contratación, no pudiendo transferir esa responsabilidad a otras entidades ni terceros en general.

Así también es responsable por la calidad ofrecida y por los vicios ocultos de los bienes ofertados por un plazo de un (01) año contado a partir de la conformidad otorgada, de acuerdo a lo dispuesto en el artículo 40° de la Ley de Contrataciones del Estado

11. PERFIL DEL POSTOR

- ✓ El postor deberá estar inscrito en el Registro Nacional de Proveedores (RNP).
- ✓ El postor no deberá estar impedido para contratar con el Estado Peruano.
- ✓ Los profesionales titulados propuestos deberán estar colegiados y habilitados al inicio de su participación efectiva en la ejecución del contrato, según corresponda.

12. PERSONAL CLAVE

Un (01) Jefe de Proyectos

Perfil:

- ✓ Profesión:
  Deberá tener Título Profesional de Ingeniero Electrónico o Título Profesional de Ingeniero de Sistemas o Título Profesional de Ingeniero en Computación o Título Profesional de Ingeniero en Telemática o Título Profesional de Ingeniero en Informática o Título Profesional de Ingeniero de Telecomunicaciones.

- ✓ Capacitación:
  Deberá tener un curso o especialización o diplomado o post grado o maestría en: gestión proyectos o dirección de proyectos o gerencia de proyectos o gestión de proyectos TI; o tener la certificación PMP (Project Management Profesional) vigente o PRINCE2 Practitioner Certificate.

Funciones:

- Responsable de la Gestión del Proyecto.
- Realizar las coordinaciones y seguimiento necesario para la ejecución del proyecto en el

plazo solicitado por el SENCICO y minimizando los riesgos de operación de este servicio.

- Reportar cualquier incidencia o restricción en el proyecto, que no permita la continuidad del proyecto, de forma inmediata al SENCICO.
- Presentar reportes semanales de avance.
- Presentar cronogramas semanales actualizados.
- Presentar actas de reuniones.
- Presentar el informe final y entregables definidos.
- Firma la documentación del proyecto, como: Actas de reunión, Acta de conformidad, Informes, Protocolo de pruebas, Hojas de trabajo, etc.

El perfil deberá ser acreditado para la suscripción del contrato, con copia simple de los documentos.

Un (01) Especialista en Redes

Perfil:

- ✓ Profesión:
  Deberá tener Título Profesional de Ingeniero Electrónico o Título Profesional de Ingeniero de Sistemas o Título Profesional de Ingeniero en Computación o Título Profesional de Ingeniero en Telemática o Título Profesional de Ingeniero en Informática o Título Profesional de Ingeniero de Telecomunicaciones o Bachiller en Ingeniería Electrónica o Bachiller en Ingeniería de Sistemas o Bachiller en Ingeniería de Computación o Bachiller de Ingeniería en Telemática o Bachiller en Ingeniería de Informática o Bachiller en Ingeniería de Telecomunicaciones.

- ✓ Capacitación:
  Deberá tener una Certificación Oficial Nivel Profesional vigente en la marca propuesta de los equipos LAN, WLAN y soluciones de software ofrecidos.

El perfil deberá ser acreditado para la suscripción del contrato, con copia simple de los documentos.

Funciones:

- Responsable de la instalación y configuración de los equipos LAN y WLAN.
- Responsable de la supervisión del mantenimiento preventivo y correctivo de los equipos LAN y WLAN.
- Realizar las coordinaciones técnicas para la instalación y configuración de los equipos LAN y WLAN.
- Absolver las consultas técnicas, realizadas por el Departamento de Informática.
- Resolver en conjunto con SENCICO cualquier incidencia o restricción o técnica de configuración, que no permita la continuidad del proyecto, de forma inmediata al SENCICO.
- Responsable técnico de la ejecución del protocolo de pruebas y/o hojas de trabajo de los equipos LAN y WLAN.
- Firma en la documentación del proyecto, como: Actas de reunión, Acta de conformidad, Informes, Protocolo de pruebas, Hojas de trabajo (Checklist), etc. referente a los equipos LAN y WLAN.

Un (01) Especialista en Servidores de Comunicaciones

Perfil:

- ✓ Profesión:
  Deberá tener Título Profesional de Ingeniero Electrónico o Título Profesional de Ingeniero de Sistemas o Título Profesional de Ingeniero en Computación o Título Profesional de Ingeniero en Telemática o Título Profesional de Ingeniero en Informática o Título Profesional de Ingeniero de Telecomunicaciones o Bachiller en Ingeniería Electrónica o Bachiller en Ingeniería de Sistemas o Bachiller en Ingeniería de Computación o Bachiller de Ingeniería en Telemática o Bachiller en Ingeniería de Informática o Bachiller en Ingeniería de Telecomunicaciones.

- ✓ Capacitación:
  Deberá tener una Certificación Oficial Nivel profesional vigente, en la marca propuesta de los equipos de comunicaciones y soluciones de software ofrecidos.

El perfil deberá ser acreditado para la suscripción del contrato, con copia simple de los documentos.

Funciones:

- Responsable de la instalación y configuración de los equipos de gestión y administración de Comunicaciones.
- Responsable de la supervisión del mantenimiento preventivo y correctivo de los Servidores de Comunicaciones.
- Realizar las coordinaciones técnicas para la instalación y configuración de los Servidores de Comunicaciones.
- Absolver las consultas técnicas, realizadas por el Departamento de Informática.
- Resolver en conjunto con SENCICO cualquier incidencia o restricción o técnica de configuración, que no permita la continuidad del proyecto, de forma inmediata al SENCICO.
- Responsable técnico de la ejecución del protocolo de pruebas y/o hojas de trabajo.
- Firma en la documentación del proyecto, como: Actas de reunión, Acta de conformidad, Informes, Protocolo de pruebas, Hojas de trabajo (Checklist), etc.

13. LUGAR DE ENTREGA

Los bienes serán entregados en el Almacén de la Sede Central (Av. De La Poesía Nº 351 – San Borja - Lima), para la verificación del cumplimiento de las características técnicas, de lunes a viernes de 8:30 am a 1:00 pm y de 2:00 pm a 4:00 pm, y luego de ello el Contratista recogerá los equipos para proceder a instalarlos en los locales de las Sedes Zonales, para los que corresponda, previa coordinación con el Departamento de Informatica y cada Sede Zonal, dentro del plazo de implementación.

N°	Sedes	Dirección
1	**GZ AREQUIPA**	Sede Grau: Calle Puente Grau Nº 325 - Cercado Arequipa Sede Yanahuara: León Velarde, 407 - Yanahuara - Arequipa, Arequipa
2	**GZ CHICLAYO**	Av. Juan Tomis Stack N° 980 Urb. El Ingeniero I – Chiclayo (frente al GOBIERNO REGIONAL) Chiclayo, Chiclayo, Lambayeque
3	**GZ CUSCO**	Av.Tomasa Titto Condemayta Nº 411-Wanchaq Wanchaq, Cusco, Cusco -
4	**CF LOS OLIVOS**	Av. Alfredo Mendiola 4203 Los Olivos, Lima, Lima -
5	**GZ PIURA**	Av. Grau 1535 Piura, Piura, Piura
7	**GZ TRUJILLO**	Av. Carlos Monge 292 Urb. Chimú Trujillo, Trujillo, La Libertad
6	**CF SAN BORJA Y SEDE CENTRAL**	Av. De la Poesía 351 San Borja, Lima, Lima

14. PLAZO DE ENTREGA

A. Prestación principal:

El plazo de entrega de los Equipos de comunicaciones LAN y WAN, será de la siguiente manera.

Actividad	Plazo máximo	
Entrega de los bienes	45 días calendarios	Contabilizados a partir del día siguiente de suscrito el Contrato. ***Entrega almacén Sede Central**
Implementación de los	60 días	Contabilizados a partir del día siguiente de

Equipos de comunicaciones LAN	calendarios	aprobado el Plan de Trabajo. **Incluye recojo de almacén sede central y distribución de equipos a las Sedes Zonales.*

B. Prestaciones Accesorias:

Actividad	Plazo Máximo
Mantenimiento Preventivo y correctivo	1er Mantenimiento preventivo y correctivo: dentro de los quinientos (500) días calendarios, como máximo, contabilizados a partir del día siguiente de firmado el Acta de Aceptación de la implementación de los Equipos de comunicaciones LAN. 2do Mantenimiento preventivo y correctivo: dentro de los novecientos cincuenta (950) días calendarios, como máximo, contabilizados a partir del día siguiente de firmado el Acta de Aceptación de la implementación de los Equipos de comunicaciones LAN.
Soporte Técnico	Durante los un mil noventa y cinco (1095) días calendarios, contabilizados desde el día siguiente de firmado el Acta de Aceptación de la Infraestructura Tecnológica (Equipos de comunicaciones LAN).
Capacitación	Dentro de los sesenta (60) días calendarios, contabilizados desde el día siguiente de suscrito el Contrato.

15. GARANTIA

La garantía será de un mil noventa y cinco (1095) días calendarios días calendario, contabilizados a partir del día siguiente de firmado el Acta de Aceptación de la implementación de los equipos de comunicaciones del presente Contrato.

16. CONFORMIDAD DE LOS BIENES

Será otorgada por el Departamento de Informática a través de la verificación del cumplimiento de las condiciones contractuales, según lo establecido en el artículo 168° del Reglamento de la Ley de Contrataciones del Estado, en un plazo que no excederá de los siete (07) días calendarios de recepcionado el entregable, de acuerdo a lo dispuesto en el Decreto Supremo N° 168-2020-EF.

De existir observaciones, el Asesor de Sistemas e Informática comunicará al contratista, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (02) ni mayor de ocho (08) días calendarios, dependiendo de la complejidad; de acuerdo a lo dispuesto en el Decreto Supremo N° 168-2020-EF. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, EL SENCICO podrá resolver el contrato, sin perjuicio de aplicar las penalidades que correspondan.

Se comunicará las observaciones al Contratista, mediante documento, en un plazo máximo de siete (07) días calendarios, contabilizados a partir del día siguiente de recepcionado el entregable.

17. ENTREGABLES

Los entregables se detallan a continuación:

PRESTACIONES	ENTREGABLES	PERIOCIDAD
Prestación Principal	El Contratista deberá presentar a los tres (03) días calendarios, contabilizados a partir del día siguiente de culminado el plazo de **Implementación del equipo de comunicaciones LAN y WLAN**, un Informe Final (digital) que contenga lo siguiente: ➢ Memoria descriptiva de los trabajos realizados y de la implementación. ➢ Topología Final Implementada (formato Visio) ➢ Especificaciones técnicas de todos los equipos implementados. ➢ Reporte fotográfico de los equipos y gabinetes, las fotos	Una sola vez

	deben ser frontales y posteriores, donde se visualice claramente que la instalación se ha realizado correctamente y que el equipo cuente con las etiquetas correspondientes; así como todos los componentes instalados. ➢ Layout de gabinetes donde se ha instalado el equipo, incluyendo todos los equipos y componentes que alberga dicho Gabinete. Así mismo el Layout deberá contar con la dirección IP del Equipo, MAC Address, Hostname y Número de Serie, en formato Visio o AutoCAD. ➢ Una ficha detallada de la configuración de cada equipo (switch, ap, servidores de comunicaciones), indicando el nombre, IP, número de serie, Mac Address, control patrimonial, conexiones, así como los servicios que se ejecutan en él. ➢ Show run de los Switches y pantallas de configuración de los servidores de comunicaciones y AP. ➢ Nomenclatura de rotulación de equipos, en formato Excel. ➢ Port Mapping del Switch en formato Excel. ➢ Procedimiento de atención para el soporte técnico, con niveles de escalamientos. ➢ Protocolo de prueba, debidamente firmados por el Contratista y SENCICO. ➢ Documento Excel de inventario de equipos indicando código patrimonial, sede, dependencia, ubicación, nombre equipo, número de serie, puerto de enlace. ➢ Carta de garantía de fábrica de todos los equipos solicitados en el presente proceso, donde se indique marca, modelo, número de serie y partes/componentes del equipo correspondiente. Así mismo en esta carta se debe precisar que los equipos son de primer uso y de año de fabricación 2020.	
Prestación Accesoria	**Mantenimiento Preventivo y Correctivo** El Contratista deberá presentar a los tres (03) días calendarios, contabilizados a partir del día siguiente de culminado cada Mantenimiento Preventivo y Correctivo, un Informe Final (digital) que contenga lo siguiente: ➢ Informe del mantenimiento: Actividades preventivas realizadas ➢ Hoja de trabajo (Checklist), firmado por el personal que ejecuto el mantenimiento, supervisor del Contratista y supervisor de SENCICO. ➢ Backup digital de configuración de todos los equipos de comunicaciones del presente Contrato. ➢ Reporte Fotográfico, de los equipos y gabinetes, las fotos deben ser frontales y posteriores, donde se visualice claramente que la instalación se ha realizado correctamente y que el equipo cuente con las etiquetas correspondientes; así como fotos todos los componentes. ➢ Topología de Red en formato Visio. ➢ Layout de gabinetes, incluyendo todos los equipos y componentes que alberga dicho Gabinete. Así mismo el Layout deberá contar con la dirección IP del Equipo, MAC Address, Hostname, Código patrimonial y Numero de Serie, en formato Visio o AutoCAD. ➢ Nomenclatura de rotulación de equipos, en formato Excel. ➢ Port Mapping del Switch en formato Excel. ➢ Protocolo de pruebas realizadas luego de reestablecer el servicio, la cual deberá estar firmado por el Supervisor del Mantenimiento en CAMPO por parte de SENCICO y el Personal del Contratista que realizo las actividades en Situ.	Dos veces, de acuerdo al Ítem 14, plazo de entrega.

	➢ Diagnóstico y acciones correctivas recomendadas referente a los equipos de comunicaciones. ➢ Recomendaciones finales a nivel de equipamiento, arquitectura, configuración e infraestructura. ➢ Documento Excel de inventario de equipos indicando código patrimonial, sede, dependencia, ubicación, nombre equipo, número de serie, puerto de enlace. ➢ Informe de obsolescencia tecnológica (EOS y EOL) de cada equipo con las recomendaciones del fabricante.	
	Soporte Técnico: El Contratista deberá presentar a los cinco (05) días calendarios, contabilizados a partir del día siguiente de culminado el periodo mensual de soporte, un Informe mensual (digital) que contenga el consolidado de Incidentes presentados y atendidos en el periodo trimestral, recomendaciones y conclusiones.	Mensual
	Capacitación El Contratista deberá presentar a los tres (03) días calendarios, contabilizados a partir del día siguiente de concluida la capacitación, de manera digital, lo siguiente: ✓ Documento de Asistencia de los participantes, donde se indique el nombre, el día y la firma del participante. ✓ Constancia o certificado del curso, a todos los asistentes, donde especifique el nombre y apellido del personal participante, fecha y duración del curso, debiendo estar firmado por el capacitador.	Una sola vez

18. FORMA DE PAGO

El pago se realizará de acuerdo al siguiente cuadro:

PRESTACIONES		PAGO
Prestación Principal	Entrega del Bien	Único pago: 100%
	Implementación de los equipos de comunicación LAN y WLAN	Único pago: 100%
Prestación Accesoria	Mantenimiento Preventivo y Correctivo	Dos pagos: 50% - 1er mantenimiento 50% - 2do mantenimiento
	Soporte Técnico	Pagos trimestrales: - 12 pagos iguales
	Capacitación	Único pago: 100%

El pago se efectuará mediante el respectivo abono en la cuenta bancaria individual del postor ganador, en un plazo de diez (10) días calendarios, de acuerdo a lo dispuesto en el Decreto Supremo N° 168-2020-EF, de encontrase completo el expediente de pago, sea a través del Banco de la Nación o de cualquier otra institución bancaria del Sistema Financiero Nacional, para cuyo efecto EL CONTRATISTA comunicará su CODIGO DE CUENTA INTERBANCARIO (CCI).

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Recepción del bien (solo para la prestación principal, presentar guía de remisión, donde se detalle cada componente del bien y su número de serie)
- Conformidad del área usuaria.
- Comprobante de pago.
- Entregable correspondiente de la prestación principal y/o accesoria.

19. PENALIDADES APLICABLES

En caso de retraso en la ejecución de las contraprestaciones ejecutadas por el contratista, se

aplicará una penalidad al contratista por cada día de retraso hasta por el monto máximo del 10% del monto según lo dispuesto en los artículos 161º y 162º del Reglamento de la Ley de Contrataciones del Estado vigente.

20. OTRAS PENALIDADES

De conformidad con lo estipulado en el artículo 163° del Reglamento de la Ley de Contrataciones del Estado, se han establecido otras penalidades diferentes a la penalidad por mora, las cuales son objetivas, razonables y congruentes con el objeto de la convocatoria, las mismas que se detallan a continuación:

N°	Supuesto de aplicación de penalidad	Monto aplicable S/	PROCEDIMIENTO
1	Incumplir con el plazo de entrega del PLAN DE TRABAJO de Implementación de la Infraestructura Tecnológica.	300.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de entrega del Plan de Trabajo, la penalidad será aplicada.
2	Incumplir con el plazo de presentación de Informe Final de implementación.	500.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de entrega del Informe Final de implementación, la penalidad será aplicada
3	Incumplir con el plazo de presentación de Informe mensual de incidencias.	200.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de entrega del Informe mensual de incidencia, la penalidad será aplicada
4	Incumplir con el plazo de presentación de Informe final de mantenimiento.	200.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de entrega del Informe Final de mantenimiento, la penalidad será aplicada
5	Incumplir con "no lograr restablecer el servicio a partir de terminado el mantenimiento, el CONTRATISTA deberá realizar las acciones necesarias con la finalidad de solucionar los problemas presentados en un lapso no mayor de cuatro (04) horas contadas a partir de reportado el problema, (…)"	500.00	Por cada 1 (una) hora excedente que el contratista incumpla con el plazo de cuatro (04) horas contadas a partir de reportado el problema, la penalidad será aplicada.
6	Incumplir con el SLA: Tiempo máximo de resolución de incidencia s/cambio de equipo y/o componente: 4 horas, para Lima, Lima Switchs de Core y Provincia.	200.00	Cada vez que el contratista incumpla el SLA: *"Tiempo máximo de resolución de incidencia s/cambio de equipo y/o componente: 4 horas",* la penalidad será aplicada.
7	Incumplir con el SLA: Tiempo máximo de resolución de incidencia c/cambio y/o componente de equipo: 12 horas, para el Switchs de Core (N°20 de la lista).	300.00	Cada vez que el contratista incumpla el SLA: *"Tiempo máximo de resolución de incidencia c/cambio de equipo y/o componente: 12 horas",* la penalidad será aplicada.
8	Incumplir con el SLAs: Tiempo máximo de resolución de incidencia c/cambio y/o componente de equipo: 24 horas (lima).	400.00	Cada vez que el contratista incumpla el SLA: *"Tiempo máximo de resolución de incidencia c/cambio de equipo y/o componente: 24 horas",* la penalidad será aplicada.
9	Incumplir con el SLAs: Tiempo máximo de resolución de incidencia c/cambio y/o componente de equipo: 48 horas (provincia).	500.00	Cada vez que el contratista incumpla el SLA: *"Tiempo máximo de resolución de incidencia c/cambio de equipo y/o componente: 48 horas"*, la penalidad será aplicada.
10	Cambio del Personal Clave	500.00	Cada vez que el Contratista cambie el

			Personal Clave, sin comunicar a la Entidad por Mesa de Partes al Departamento de informática, la penalidad será aplicada.
11	Ingreso no autorizado a la red y/o sistemas y/o equipos de SENCICO	3000.00	Cada vez que el Contratista ingrese a la Red y/o equipos y/o sistemas, de manera no autorizada, la penalidad será aplicada.

El procedimiento para comunicar las penalidades, es la siguiente:

- El área usuaria es el responsable de comunicar al Contratista, mediante Carta con copia al Departamento de Abastecimiento, los incumplimientos u omisión de obligaciones, como máximo a 07 días calendarios de ocurrido el incidente.
- El Contratista en un plazo no mayor a 07 días calendarios, contabilizados desde el día siguiente de recepcionado la Carta de Incidente, realizará su descargo correspondiente a través de mesa de partes virtual: https://app.sencico.gob.pe/prd/waMesaPartes/MesaPartes, en el horario de lunes a viernes de 8:30am a 5:00pm) de SENCICO, después de las 5:00pm, se considerará el documento con fecha del siguiente día útil.
- El área usuaria, comunicará oportunamente al Departamento de Abastecimiento, para la aplicación de la Penalidad, en caso corresponda.

21. CONFIDENCIALIDAD

El contratista se compromete a mantener en reserva, y no revelar a terceros, sin autorización escrita de SENCICO, la información que le sea suministrada por este último o a la cual tenga acceso, excepto en cuanto resultare estrictamente necesario para el cumplimiento del Contrato, y que restringirá la revelación de dicha información sólo a sus empleados, sobre la base de "necesidad de conocer".

En el bien y con el fin de resguardar la información de la entidad se prohíbe las siguientes actividades:

- Se prohíbe que el Contratista utilice softwares para capturar información de la Entidad, en caso se detecte que el Contratista tenga instalado un software de captura de información, este será retirado inmediatamente de la Entidad.
- Se prohíbe que el Contratista ingrese sin autorización y supervisión del Departamento de Informática, a la red y/o equipos y/o sistemas de la Entidad.

22. REQUISITOS DE CALIFICACIÓN

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 2,000,000.00 (dos millones 00/100 soles) por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran bienes similares a los siguientes: adquisiciones de equipos de redes, o adquisición de equipos de comunicaciones o adquisición de equipos de telecomunicaciones o adquisición de un sistema de redes o adquisición de red LAN. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito,

nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[1], correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad.

En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad.

Importante
En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".

[1] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

> *"… el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*
> *(…)*
> *"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.1	**EXPERIENCIA DEL PERSONAL CLAVE**

Requisitos:

Jefe de Proyectos:
Deberá contar con una experiencia mínima de tres (03) años como Jefe de Proyectos o Gestor de proyecto o Gerente de Proyecto o Coordinador de Proyectos en la especialidad de: Telecomunicaciones o Redes o Networking o Infraestructura Tecnológica del personal clave requerido como Jefe de Proyectos.

Especialista en Redes:
Deberá contar con una experiencia mínima de dos (02) años en labores relacionadas con la configuración o implementación o instalación o mantenimiento o soporte de: equipos de comunicaciones o equipos de telecomunicaciones o equipos de networking o equipos de redes, del personal clave requerido como Especialista en Redes.

Especialista en Servidores de Comunicaciones:
Deberá contar con una experiencia mínima de dos (02) años en labores relacionadas con la configuración o implementación o instalación o mantenimiento o soporte de: equipos de comunicaciones o equipos de telecomunicaciones o equipos de networking o equipos de redes o equipos servidores de comunicaciones, del personal clave requerido como Especialista en Servidores de Comunicaciones.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- *El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.*
- *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.*
- *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.*
- *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*
- *El cumplimiento de las Especificaciones Técnicas se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de las características y/o requisitos funcionales. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*
- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*

FIRMA DIGITAL
Firmado digitalmente por: VARAS GRAUS Roger Hector FAU 20131377810 soft
Motivo: Soy el autor del documento
Fecha: 17/11/2020 16:49:55-0500

Firmado digitalmente por: CHUQUILLANQUI BARRIENTOS Jorge Luis FAU 20131377810 soft
Motivo: Soy el autor del documento
Fecha: 17/11/2020 15:58:21-0500