SERVICIO DE RENTAS INTERNAS

Programa de Mejoramiento del Servicio de Rentas Internas EC-L1120
Préstamo BID 3325/OC-EC
LICITACIÓN PÚBLICA INTERNACIONAL No. PA-2019-007
"INFRAESTRUCTURA DE RED PARA EL DATA CENTER PRINCIPAL Y AGENCIAS"

BOLETÍN DE ENMIENDAS No. 2

Enmienda 1:

Parte II. Sección VII. Requisitos de los bienes y Servicios. Especificaciones Técnicas, páginas 177 - 199:

Bajo el título "Elementos de Hardware", se reemplazan íntegramente las especificaciones técnicas mínimas requeridas de cada uno de los 12 ítems, por las siguientes:

En adelante dirá:

ITEM 1: SWITCH DE ACCESO DE CAPA TRES DE 48 PUERTOS

Equipo: Switch de Acceso de capa tres de 48 Puertos para agencias	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	Switch Capa 3 de alto rendimiento con Uplinks de al menos 10Gbps El tamaño del equipo deberá ser de 1 RU.
Marca	De la misma marca de los switch Spine y Leaf para Data Center, indicados en los ítems 5, 6, 7 y 8
Licenciamiento	Cada equipo debe estar registrado en el sistema Prime o en el sistema de gestión ofertado y administración esencial para consola centralizada o que se pueda integrar usando un SNMP AGENT (compatible con CISCO PRIME).
	Cada equipo debe incluir licenciamiento para recolección de flujos (al menos 500 flujos de cada switch) y su registro respectivo en el sistema Prime o en el sistema de gestión ofertado.
Compatibilidad	El switch propuesto y todas sus funcionalidades de control de acceso deben ser compatibles con el software de seguridad de control de acceso ofertado.
	Las políticas de seguridad del switch se deben poder establecer desde el software de seguridad de control de acceso ofertado.
Especificaciones generales mínimas	El switch propuesto debe contar con, al menos, las tecnologías de siguiente generación que se listan a continuación: – Listas de Acceso en capa 2 y capa3 – Calidad de Servicio QoS en capa 2 y capa 3
	El switch propuesto debe tener una CPU con al menos 2 (dos) GB de memoria RAM
	El switch propuesto debe contar con, al menos, 48 (cuarenta y ocho) puertos 10/100/1000.
	El switch propuesto debe ser PoE y cumplir al menos los siguientes requisitos sobre la energía que puede entregar: – Debe poder ofrecer, al menos, 15 (quince) W por puerto en, al menos, 48 (cuarenta y ocho) puertos de forma simultánea. – Debe contar con al menos 1152 (mil ciento cincuenta y dos) W disponibles para PoE.
	El switch propuesto debe ofrecer, al menos, el siguiente rendimiento: – Capacidad de conmutación: al menos 256 (doscientos cincuenta y seis) Gbps. – Capacidad de transmisión: al menos 144 (ciento cuarenta y cuatro) Mbps.
	El switch propuesto debe poder manejar, al menos, 4000 (cuatro mil) identificadores de VLANs

	El switch propuesto debe trabajar con VxLAN. Si es necesario, en la arquitectura propuesta se debe colocar un equipo adicional (en al menos 5 agencias) con la capacidad de operar con VxLAN entre las agencias. Esta característica debe venir totalmente licenciada y operativa.
	El switch propuesto debe poder manejar jumbo frames con un tamaño mínimo de 9198 bytes.
	El switch propuesto debe tener, al menos, 2 (dos) fuentes de poder. Estas fuentes deben poder ser reemplazadas (Hot-pluggable) o intercambiables (hot-swappable) en caliente.
	El switch propuesto debe contar con, al menos, los siguientes mecanismos de QoS: – 802.1p CoS (Class of Service). – Clasificación DSCP (Differentiated Services Code Point). – Debe incluir mecanismos de encolamiento de tráfico – CIR (Committed Information Rate). – Debe incluir mecanismos estándar de encolamiento de tráfico en momentos de congestión – Manejo de prioridad a nivel de colas, ocho colas de salida por puerto basado en hardware, debe de incluir al menos dos colas de prioridad. – Marcado y clasificación de paquetes basado en dirección IP origen y destino, MAC origen y destino y numero de puertos TCP y UDP.
ESPECIFICACIONES DE FUNCIONALIDADES Y SERVICIOS	
Protocolos	El switch propuesto debe poder enrutar el tráfico mediante cualquiera de los siguientes protocolos estándar: – RIP routed access – OSPF routed access – IS – IS – Policy based routing – VRRP (Virtual router redundancy protocol)
	Soporte de Spanning Tree IEEE 802.1d así como las mejoras tales como convergencia rápida (RST 802.1w) y múltiples instancias (MST 802.1s).
	Capacidad de operación de puertos en al menos full dúplex
	Soporte de NTP, IGMP y ahorro de energía mediante Energy Efficient Ethernet (EEE)
	Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad
	Puertos de consola: RJ45 y puerto ethernet 10/100 dedicado para administración fuera de banda. Se acepta la posibilidad de que cualquiera de estos puertos puedas ser provistos a través de transceiver.
	Registro de eventos vía Syslog
	Debe permitir administración vía web.
	Debe tener múltiples niveles de privilegios de acceso (mínimo 2) por puerto de consola o Telnet para administración.
	Para asegurar una óptima seguridad en la gestión, se debe de poder colocar filtros de acceso que sólo permitan el acceso a determinadas IP en los puertos de gestión.
	El switch debe soportar procesos de debug para análisis en caso de fallas
	El switch debe tener la capacidad de limitar la cantidad de direcciones MAC aprendidas en un puerto para evitar ataques MAC address flooding que llenen la tabla de direcciones MAC del switch.
	Soporte de mecanismos para evitar ataques tipo DoS (denegación de servicio) y spoofing.
	Filtros aplicables por puerto, filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP
	Soporte de autenticación 802.1x con asignación dinámica de VLAN y asignación dinámica de listas de control de acceso (ACL).
	Control de acceso centralizado por RADIUS, tanto para los administradores del switch como para los usuarios de la red que se autentican según estándar IEEE 802.1x.
	Soporte de movilidad de MAC en esquemas de 802.1x detrás de un teléfono, permitiendo

	que al ser autenticado el usuario conectado a un teléfono y luego de su desconexión, el switch pueda recibir información de la desconexión a pesar de no estar el usuario físicamente conectado al switch, evitando el spoofing de la MAC.
	Soporte de 802.1x, autenticación por MAC (MAB) y Web Authentication de manera dinámica para usuarios que se conectan detrás del teléfono.
	Análisis de tráfico usando protocolos tipo Netflow o similares (como Openflow, Sflow). El análisis de tráfico debe de ser tanto en el downlink como en el uplink.
	Soporte de "port mirroring" por puerto y por VLAN.
	Soporte de múltiples sesiones de "port mirroring" así como "port mirroring" remoto.
Escalabilidad	El switch propuesto debe tener una memoria buffer para paquetes de, al menos, 4 (cuatro) MB.
	El switch propuesto debe soportar dual-stack IPv4/IPv6 para facilitar la migración de IPv4 a IPv6.
	El switch propuesto debe poder crecer en número de puertos mediante módulos opcionales. El crecimiento debe ser posible tanto en puertos de 1Gbps,10 Gbps, o 40 Gbps
	Los switches requeridos deben soportar la formación de stacks entre ellos: – El stack debe soportar al menos 8 (ocho) switches. – El ancho de banda mínimo, dedicado para el stack, debe ser al menos 80 (ochenta) Gbps. – Se debe poder agregar o retirar miembros al stack
	El switch debe soportar al menos 32,000 (treinta y dos mil) direcciones MAC
Seguridad	El switch propuesto debe soportar el uso de algoritmos avanzados de análisis de comportamiento; que permitan identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos. Esta funcionalidad debe estar activada en los equipos adicionales de cada agencia (al menos 5) con su respectiva licencia de funcionamiento y todo el hardware necesario para realizarlo.
Requerimientos especificos operativos	Cada fuente de poder del switch propuesto debe poder trabajar con energía alterna (AC) en el rango desde los 100 (cien) hasta los 240 (doscientos cuarenta) V.
	Cada switch propuesto se debe poder montar en un rack de comunicaciones de 19" y ocupar un espacio que no supere 1 (una) RU (Rack Unit).
Funcionalidades avanzadas	Cada equipo propuesto debe contar con funcionalidades avanzadas de al menos, 3 (tres) años que incluya lo siguiente: – Características de automatización: ➢ Plug and Play: el equipo debe ser dado de alta automáticamente por la controladora central o el software de gestión ➢ Plantillas de configuración ➢ Obtención de información de inventario de los equipos ➢ Obtención de la topología de la red ➢ Administración de versiones de software: estandarización de imágenes de software, verificaciones antes y después de realizar el despliegue de nuevas versiones de software en los switches. ➢ Generación de grupos de dispositivos para simplificar tareas administrativas ➢ Generación de reportes ➢ Ejecución de scripts usando Python o similares (de forma centralizada o en el switch) ➢ El switch debe automatizar las siguientes funciones mediante el uso de la interfaz gráfica del controlador Software Defined: ▪ Despliegue de políticas de Calidad de Servicio (QoS) de manera automatizada en base al listado de aplicaciones criticas, no criticas y por defecto para el SRI o perfiles de usuarios asignados por el SRI ▪ Gestión centralizada de la instalación de actualizaciones criticas en los switches (patching) ▪ Segmentación automatizada basada en politicas de usuarios. La segmentación de usuarios debe poder hacerse en base a sus respectivos roles en la organización. La configuración de estas politicas debe poder

	hacerse en un entorno gráfico, de manera centralizada. ▪ El software del switch debe permitir plug and play, zero touch provisioning. – Características de monitoreo y aseguramiento de servicios: ➢ Visión completa que incluya al menos: analítica con respecto a la salud del equipo, problemas que se presentan en los switches, que ayude a la resolución del inconveniente. ➢ Obtención del path de tráfico de manera gráfica en la interfaz gráfica de usuario del controlador SDN o del sistema de analítica ofertado. El path de tráfico mostrado debe proporcionar información con respecto a los dispositivos, interfaces y políticas de calidad de servicio involucradas en el path de tráfico de interés.. ➢ Analíticos con respecto a la salud o diagnóstico de los usuarios conectados en la red. El switch debe soportar las siguientes funciones de monitoreo y aseguramiento de servicios, mediante el uso de la interfaz gráfica de la controladora central, o el software de gestión o el componente de analítica ofertado como parte de la solución: ▪ Performance de las aplicaciones que pasan a través del switch.. ▪ Visualización de problemas globales que incluyan múltiples dispositivos ▪ Monitoreo del plano de datos, control y políticas de los switches
Funcionalidades avanzadas (continuación)	➢ Búsqueda de usuarios conectados a los switches ➢ Ubicación geográfica de los switches ➢ Correlación de la información recopilada del switch (SNMP, syslog, netflow o similares) para acelerar la resolución de problemas.

ITEM 2: ACCESS POINTS

Equipo: Puntos de Acceso Inalámbrico para agencias	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	Punto de acceso inalámbrico para instalarse en interiores con antenas internas, manejado a través de controladora inalámbrica.
Especificaciones generales mínimas	Los access points se instalarán en interiores, deben contar con antenas internas embebidas.
	Los Access points deben ser controlados por la controladora inalámbrica con la que cuenta la institución o por la nueva controladora ofertada en este proceso
	Soporte para PoE+ (802.3at), a través del puerto de red y mediante power injector
	Al menos 1 interfaz 100/1000BASE-T autosensing (RJ-45)
	Un puerto de consola (RJ-45) o usb
	Para la gestión de equipos, cada access point debe contar con 17 licencias assurance para reconocimiento de cisco prime. En caso de Ofertar otra solución de gestión centralizada, se debe incluir en la oferta el licenciamiento para gestionar al menos 235 equipos de red
Funcionalidades Básicas	El access point debe contar con 2 radios: el primero debe operar en 5 Ghz y el segundo debe poder operar en 5 Ghz y/o en 2.4 Ghz
	El access point debe cambiar, el modo de operación de los radios de servicios basado en el entorno de radio frecuencia (RF). El equipo debe soportar los siguientes modos de operación: - Modo 2.4 Ghz y 5 Ghz: Un radio atiende clientes en la banda 2.4 Ghz y el otro radio atiende clientes en la banda de 5 Ghz. - Modo 5 Ghz y monitoreo: Un radio sirve a clientes en la banda de 5Ghz, mientras el otro está escaneando el espectro en busca de amenazas (WIPS), interferencias y access points no administrados.
	El access point debe soportar beamforming tanto en la comunicación cliente-access point como en la comunicación access point-cliente; sin requerir ninguna capacidad

	especial en el dispositivo cliente. Esto debe ser soportado para clientes con 802.11a/b/g/n/ac
	El Access point debe tener hardware dedicado o utilizar las técnicas con los mismos radios que tiene para analizar el espectro y detectar interferencias.
	Soporte para optimización de ambientes de alta densidad de al menos 200 usuarios
	El punto de acceso se enviará con soporte para la sujeción en pared
	Soporte para 802.11 AC wave 2 con 3 streams espaciales MU-MIMO.
Estándares soportados	IEEE 802.11a/b/g/n/ac/acw2, 802.11h, 802.11d
Desempeño	Potencia de Tx (2.4GHz/5 Ghz) de al menos 22 dBm (200 mW)
	Radio Flexible (puede funcionar en 2.4 Ghz y/o 5 Ghz): - 2.4 GHz: antena interna con ganancia de al menos 3 dBi, omnidireccional
	Radio dedicado 5Ghz 5 Ghz: antena interna con ganancia de al menos 3 dBi, omnidireccional en azimuth
Seguridad	Advanced Encryption Standards (AES).
	802.11i, Wi-Fi Protected Access 2 (WPA2), WPA
	802.1X
	Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).
	EAP-Tunneled TLS (TTLS) o Microsoft Challenge Handshake Authentication Protocol Versión 2 (MSCHAPv2).
	Protected EAP (PEAP) v0 o EAP - MSCHAPv2.
Funcionalidades Avanzadas	Cada equipo propuesto debe contar con funcionalidades avanzadas que le permitan a la controladora o al software de gestión, por al menos 3 (tres) años lo siguiente: ▪ Que el access point sea descubierto, configurado y gestionado por la controladora inalámbrica ofertada. ▪ Características de automatización: o Despliegue de día 0 (zero touch provisioning). ▪ El access point debe tener las siguientes funcionalidades mediante el uso de la interfaz gráfica de la controladora o el software de gestión: o Despliegue de políticas de Calidad de Servicio (QoS) de manera automatizada en base al listado de aplicaciones críticas, no criticas y por defecto para el SRI o perfiles de usuarios asignados por el SRI o Habilidad para convertir un radio de los access points en un sensor que permita monitorear de manera proactiva el performance de la red

ITEM 3: ROUTER

Equipo: ROUTER CONCENTRADOR DE ENLACES ENTIDADES EXTERNAS	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	El equipo de hardware debe disponer de fuente de alimentación redundante.
	Debe tener al menos 4 interfaces habilitadas 10/100/1000 Mbps RJ-45.
	Debe tener una capacidad de throughput de al menos 1 Gbps, con la posibilidad de crecimiento a 2 Gbps o más.
	El equipo debe ser accesible a través de SSH y de interfaz Web usando SSL.
Características funcionales	Los equipos ofertados deben integrarse a la plataforma de administración Cisco Prime Infrastructure actualmente existente en el SRI o a la consola de gestión centralizada ofertada o que se pueda integrar usando un SNMP AGENT (compatible con CISCO PRIME). Incluir el licenciamiento necesario.
	El equipo debe soportar la funcionalidad de cifrado de tráfico, balanceo de enlaces, enrutamiento dinámico, y traffic shaping.. Se debe incluir el licenciamiento necesario
	El cifrado de tráfico debe soportar al menos los siguientes algoritmos de encripción: 3DES, AES de al menos 128 bits.
	Debe soportar el protocolo de seguridad IPSec
	La solución debe ser compatible con topologías de red DMVPN o similar (como ADVPN, AutoVPN, etc.).

	El equipo ofertado debe poseer al menos 4GB de memoria RAM y 2GB de memoria FLASH.
	Debe contar con un puerto de consola RJ-45, un puerto USB

ITEM 4: CONTROLADORA PARA MONITOREO Y GESTION PARA SWITCHES Y ACCESS POINTS

Equipo: CONTROLADORA PARA MONITOREO Y GESTION DE SWITCHES Y ACCESS POINTS	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	La controladora debe ser provista en un servidor appliance o virtual con todo el licenciamiento incluido y con las especificaciones mínimas de funcionamiento exigidas por el fabricante. En caso de ser servidor appliance debe contar con al menos las siguientes características: ➢ 1 unidad de rack ➢ Capacidades embebidas de colección de telemetría de red (Flexible Netflow o similar, SNMP, Syslog) ➢ Soporte para gestión de mínimo 2.000 dispositivos de red (al menos 1.000 para access points y el resto para: routers, switches, controladoras inalámbricas) ➢ Soporte para un mínimo de 17.000 clientes. ➢ El equipo de hardware debe disponer de fuente de alimentación redundante.
	La plataforma para monitoreo y gestión debe tener la capacidad de visualizar clientes o dispositivos alámbricos e inalámbricos
	El software de la controladora debe ser del mismo fabricante que los switches y access points propuestos en este proceso, u homologado (ej tipo OEM) por el fabricante.
Monitoreo de aplicaciones	La controladora o el software de gestión debe permitir crear al menos 5 perfiles de usuarios para monitoreo y gestión de aplicaciones institucionales.
	La controladora o el software de gestión debe proporcionar visibilidad del rendimiento sobre las aplicaciones institucionales o a través del sistema de analítica propuesto
Características de monitoreo y aseguramiento de servicios	Salud General de la Red: - Resumen de la salud general de los dispositivos de red y clientes - Debe mostrar problemas en la red - Vistas por sitio, ubicación geográfica, listas o topología
	Salud de la red y clientes: - La controladora o el software de gestión debe mostrar al menos la información de perfiles de clientes, entorno RF y tiempo que tardan los usuarios en conectarse a la red y de la salud de los clientes en la conexión de red. - Resumen de la salud de la red: información con respecto a los planos de control, datos y políticas
	Vista 360 de usuarios y dispositivos - Rendimiento de la red - Identificación proactiva de cualquier problema que pudiera afectar la experiencia del usuario. - Gráfico de la topología de red a la que se está conectando el dispositivo, con el score de salud de todos los dispositivos en el path. - Línea de tiempo mediante la cual se puede regresar a un instante anterior de tiempo para visualizar: eventos críticos e información completa de usuario o dispositivo de red
	Trazabilidad - Obtención del path de tráfico de manera gráfica, en la interfaz gráfica de usuario del controlador SDN o la solución de analítica ofertada. El path de tráfico mostrado debe proporcionar información con respecto a los dispositivos, interfaces y políticas de calidad de servicio involucradas en el path de tráfico de interés.
	Correlación Wireless

	Los siguientes parámetros pueden ser correlacionados por la controladora o el software de gestión en dispositivos inalámbricos compatibles: • *Conexión de clientes a la red:* fallas de asociación, autenticación y obtención de dirección IP, exclusión de clientes, tiempos excesivos de asociación autenticación y obtención de dirección IP, conectividad al servidor DHCP y servidor de autenticación de los clientes finales
	Correlación Switching Los siguientes parámetros pueden ser correlacionados por la controladora o el software de gestión en dispositivos inalámbricos compatibles: • *Conexión de clientes a la red:* servicio DHCP para el usuario y dispositivo, servicio DNS para el usuario y dispositivo, autenticación y autorización de clientes.
Características de automatización	Wireless: La controladora o el software de gestión debe permitir configuración de: • Perfiles de red: conjunto de propiedades de red que representa a un sitio o un conjunto de ellos • Creación de SSIDs para usuarios e invitados • Soporte RF avanzado • Aprovisionamiento plug and play para access points • Soporte para access lists IP
	Deployment de sucursales: Flujos de trabajo simplificados para la automatización de equipos de borde físicos o virtuales de sucursales.
	Actualizaciones de software: La controladora o el software de gestión debe permitir configuración de: • Debe actuar como un repositorio central de imágenes de software y updates de mantenimiento (SMU) que luego podrán ser instalados en los dispositivos. • Debe permitir la estandarización de versiones de software en la red especificando la versión de software en la que deben estar los dispositivos • Chequeo antes y después del upgrade para tener más control y visibilidad del proceso de upgrade.

	Descubrimiento de equipos:
	• Escaneo de dispositivos y hosts para construir una base de datos centralizada. El escaneo de dispositivos debe poder hacerse usando al menos los siguientes protocolos o mecanismos:
	  o Link Layer Discovery Protocol para endpoints (LLDP)
	  o ARP
	  o LLDP Media Endpoint Discovery (LLDP-MED)
	  o SNMPv2c, SNMPv3

	Diseño de red y administración basada en perfiles: • Debe permitir administrar la red de manera jerárquica: sitios, áreas, edificios, pisos.
	Acceso definido por software: La controladora o el software de gestión debe permitir configuración de: • Debe permitir la segmentación basada en políticas de usuarios y dispositivos usando un fabric de red automatizado o su equivalente. • Soporte de funcionalidades que permitan el despliegue y aprovisionamiento de redes definidas por software para campus, creación de redes virtuales, dominios de fabric (overlays) de manera centralizada o su equivalente, segmentación del tráfico a través de las redes virtuales.
	Calidad de Servicio: • Despliegue de políticas de Calidad de Servicio (QoS) de manera automatizada en base al listado de aplicaciones críticas, no críticas y por defecto para el SRI o perfiles de usuarios asignados por el SRI

	Plug and Play: despliegue automático de los equipos

ITEM 5: SWITCH LEAF DE 48 PUERTOS MÍNIMO 10Gbps

Equipo: SWITCH LEAF DE 48 PUERTOS MÍNIMO 10Gbps	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	Switch de alto rendimiento con Uplinks de hasta 100 Gbps El tamaño del equipo deberá ser de al menos 1 RU con al menos 1.76 Tbps de ancho de banda
Compatibilidad	El switch propuesto y todas sus funcionalidades de control de acceso debe soportar e incluir las suscripciones de software o hardware que garanticen la implementación o integración con una solución de redes definidas por software con características de microsegmentación, cifrado de datos y seguimiento de tráfico este-oeste. El switch propuesto y todas sus funcionalidades de control de acceso deben ser administradas desde la controladora definida por software de Data Center ofertada.
Especificaciones generales mínimas	El switch propuesto debe contar con, al menos, las tecnologías de siguiente generación que se listan a continuación: • Puertos: 48 x 10Gbps BaseT • Puertos: 6 x QSFP 40/100-Gbps Ó 4 x QSFP28 100-Gbps y 2 QSFP+ 40Gbps
	El switch propuesto debe tener una CPU con al menos 2 Cores (dos), Memoria de Sistema de al menos 4GB
	El switch propuesto debe poseer un buffer del sistema de al menos 12Mb
	El switch propuesto debe contar con al menos un puerto de gestión RJ45
	Número máximo de entradas de la Lista de control de acceso (ACL): al menos 768 Ingreso y 768 Egreso
	Numero de Vlan: al menos 3,900
	Soporte de rutas ECMP
	Soporte de Link Aggregation Control Protocol (LACP)
	El switch propuesto debe soportar HSRP o VRRP
	Número de instancias de múltiples árboles de expansión (MST): al menos 32
	Se deben incluir: ▪ cables ópticos activos 100Gbps/25m por cada switch, ó ▪ 2 transceivers y 2 cables de fibra óptica de 100Gbps/25m por cada switch
Especificaciones de Software	Debe contar con mecanismos programables sobre la aplicación (API) que permita a los operadores administrar los switches.
	Debe permitir la configuración a través de scripts
	Debe soportar al menos vxlan bridging, vxlan routing
	Debe soportar multicast y unicast para crear el árbol de correlación entre los dispositivos.

ITEM 6: SWITCH LEAF DE 32 PUERTOS MÍNIMO A 40Gbps

Equipo: SWITCH LEAF DE 32 PUERTOS MÍNIMO A 40Gbps	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	Switch de alto rendimiento con Uplinks de hasta 100 Gbps El tamaño del equipo deberá ser de al menos 1 RU y 3.2 Tbps de ancho de banda
Compatibilidad	El switch propuesto y todas sus funcionalidades de control de acceso debe soportar e incluir las suscripciones de software o hardware que garanticen la implementación o integración con una solución de redes definidas por software con características de microsegmentación, cifrado de datos y seguimiento de tráfico este-oeste. El switch propuesto y todas sus funcionalidades de control de acceso deben ser administradas desde la controladora definida por software de Data Center ofertada
Especificaciones generales mínimas	El switch propuesto debe contar con al menos las tecnologías de siguiente generación que se listan a continuación:

	• 32 puertos QSFPx 40/100 Gbps y que sean adaptables a 10/25 Gbps o 10/25/50 Gbps
	El switch propuesto debe tener una CPU con al menos 2 Cores (dos), memoria de Sistema de al menos 4GB
	El switch propuesto poseer un buffer del sistema de al menos 16Mb
	El switch propuesto debe contar con al menos 1 puertos de gestión RJ45 y 1 USB
	El switch propuesto debe soportar entradas ARP
	Número de entradas de la Lista de control de acceso (ACL): al menos 768 Ingreso y 768 Egreso
	Numero de Vlan: al menos 3,900
	• El switch propuesto debe soportar instancias de enrutamiento y reenvío virtual (VRF)
	Número de rutas ECMP: al menos 32
	Soporte de Link Aggregation Control Protocol (LACP)
	El switch propuesto debe soportar HSRP o VRRP
	Número de instancias de múltiples árboles de expansión (MST): al menos 64
	Se deben incluir al menos 22 transceiver QSFP 40Gbps Bi-Di SR por cada switch como
	Se deben incluir al menos 5 transceivers 10Gbps por cada switch.
	Se deben incluir al menos: ▪ cables ópticos activos de 100Gbps/25m por cada switch ó ▪ transceivers y 2 cables de fibra óptica de 100Gbps/25m.
Especificaciones de Software	Debe contar con mecanismos programables sobre la aplicación (API) que permita a los operadores administrar los switches.
	Debe permitir la configuración a través de scripts
	Debe soportar al menos vxlan bridging, vxlan routing.
	Deberá soportar multicast y unicast para crear el árbol de correlación entre los dispositivos.

ITEM 7: SWITCH LEAF DE 48 PUERTOS MÍNIMO A 10/25 Gbps

Equipo: SWITCH LEAF DE 48 PUERTOS MÍNIMO A 10/25 Gbps	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	Switch de alto rendimiento con Uplinks de hasta 100 Gbps Ethernet. El tamaño del equipo deberá ser de al menos 1 RU con al menos 3,6 Tbps de ancho de banda Los puertos descendentes deben soportar al menos 10 y 25Gbps en Ethernet.
Compatibilidad	El switch propuesto y todas sus funcionalidades de control de acceso debe soportar e incluir las suscripciones de software o hardware que garanticen la implementación o integración con una solución de redes definidas por software con características de microsegmentación, cifrado de datos y seguimiento de tráfico este-oeste. El switch propuesto y todas sus funcionalidades de control de acceso deben ser administradas desde la controladora definida por software de Data Center ofertada
Especificaciones generales mínimas	El switch propuesto debe contar con, al menos, los siguientes parámetros que se listan a continuación: • Puertos: 48 x 10/25-Gbps SFP+ • Puertos:6 x 40/100-Gbps QSFP
	El switch propuesto debe tener una CPU con al menos 4 Cores (cuatro), Memoria de Sistema de al menos 8GB
	El switch propuesto debe poseer un buffer del sistema de al menos 16MB
	El switch propuesto debe contar con al menos 1 puerto de gestión RJ45, 1 puerto USB
	El switch propuesto debe soportar entradas ARP
	El switch propuesto debe soportar IGMP

	Número de entradas de la Lista de control de acceso (ACL): al menos 768 Ingreso y al menos 768 Egreso
	Numero de Vlan: al menos 3,900
	El switch propuesto debe soportar instancias de enrutamiento y reenvío virtual (VRF)
	Número de rutas ECMP: al menos 32
	Soporte de Link Aggregation Control Protocol (LACP)
	El switch propuesto debe soportar HSRP o VRRP
	Número de instancias de múltiples árboles de expansión (MST): al menos 64
	Se deben incluir al menos 48 SFP+ de 10G SR por cada switch
	Se deben incluir: • cables ópticos activos 100G/25m por cada switch, ó • transceivers y 2 cables de fibra óptica de 100G/25m por cada switch
Especificaciones de Software	Debe contar con mecanismos programables sobre la aplicación (API) que permita a los operadores administrar los switches.
	Debe permitir la configuración a través de scripts
	Debe soportar al menos vxlan bridging, vxlan routing.
	Deberá soportar multicast y unicast para crear el árbol de correlación entre los dispositivos.

ITEM 8: SWITCH SPINE DE 64 PUERTOS MÍNIMO A 40/100 Gbps

Equipo: SWITCH SPINE	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	Switch de alto rendimiento de hasta 100 Gbps. El tamaño del equipo deberá ser de al menos 1 RU, con al menos 6,4 Tbps de ancho de banda
Compatibilidad	El switch propuesto y todas sus funcionalidades de control de acceso debe soportar e incluir las suscripciones de software o hardware que garanticen la implementación o integración con una solución de redes definidas por software con características de microsegmentación, cifrado de datos y seguimiento de tráfico este-oeste. El switch propuesto y todas sus funcionalidades de control de acceso deben ser administradas desde la controladora definida por software para data center ofertada.
Especificaciones generales mínimas	El switch propuesto debe contar con, al menos, los siguientes parámetros que se listan a continuación: • 64 puertos 40/100Gbps QSFP28 ó 32 puertos 100Gbps y 32 40GBps • Fuentes de alimentación de CA redundantes • Bandejas de ventiladores redundantes e intercambiables en caliente • Memoria del sistema: al menos 4 GB • SSD: al menos 2GB • USB: al menos 1 puerto • Puertos de consola RJ-45: al menos 1 • Puertos de administración, al menos: (1 x 10/100/1000BASE-T ó 1 x 1 Gbps SFP +) • CPU : al menos 4 núcleos
	El Equipo debe ser parte de una arquitectura automatizada y orientada a las políticas definidas por software
	El equipo debe ser compatible con la controladora definida por software de data center ofertada, indicada en el ítem 9.
Especificaciones de Software	Debe contar con mecanismos programables sobre la aplicación (API) que permita a los operadores administrar los switches.
	Debe permitir la configuración a través de scripts
	Debe soportar al menos vxlan bridging, vxlan routing

	Deberá soportar multicast y unicast para crear el árbol de correlación entre los dispositivos.

ITEM 9: CONTROLADORA DE DATA CENTER EN CLUSTER PARA SWITCH SPINE AND LEAF

Equipo: CONTROLADORA DE DATA CENTER EN CLUSTER PARA SWITCH SPINE AND LEAF	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	La controladora debe ser provista en servidor appliance o virtual appliance. En caso de ofertar servidor appliance debe tener las siguientes características: • Clúster de al menos 3 Servidores con CPU, disco duro y memoria. • Al menos 656 puertos de Borde. • Al menos 1 unidad de rack • Al menos 2 x Procesadores Intel, con al menos 6 núcleos, y la memoria caché al menos 11 MB, DDR4, y al menos 1600 MHz • Memoria 4 x DDR4 de al menos 16 GB, RDIMM 214 MHz al menos PC4-17000 o similar, doble rango x4 con 1.2V En caso de ofrecer Virtual Appliance se debe incluir los servidores físicos necesarios para realizar la instalación del hardware y disponer de Alta Disponibilidad con la recomendación dada por el fabricante de la solución.
Funcionalidades	- Debe manejar criterios de multi-tenant o multi-inquilino y alta disponibilidad. - La solución ofertada debe soportar al menos 4 tenants o inquilinos - Debe tener resolución de problemas (troubleshooting) de aplicaciones y topología - Debe mantener una gestión centralizada que optimice el rendimiento y unifique la operación de ambientes físicos y virtuales. - Debe incluir un módulo de control centralizado que permita la integración con APIs para herramientas de programabilidad (Python o similares) y elementos activos de servicios de capa 4 a capa 7 (firewalls, balanceadores, etc.) - Debe permitir la creación de flujos de comunicación entre los usuarios finales, los elementos activos de la red (firewall, switches, balanceadores, etc.) y la relación con las aplicaciones ya sea en un ambiente físico (servidores bare metal), virtual (máquinas virtuales), híbrido o, en su caso nube pública (opcional). Dichos flujos pueden ser habilitados sin importar la ubicación física de los distintos elementos en el centro de datos - El controlador y sus redes físicas y virtuales deben soportar al menos los siguientes hypervisores: VMware, Open Stack, sin importar el nivel de licenciamiento utilizado. - Debe tener al menos TACACS+, RADIUS, y Autenticación Local, incluyendo Control de Acceso basado en Roles (RBAC). - Debe incluir la integración de servicios insertados al menos a nivel de capa L4-L7 (Firewall, Balanceadores, SSL-offload, ADC, otros) usando políticas e interfaz gráfica. - Debe soportar micro-segmentación - Debe integrar políticas de red basada en el funcionamiento de las aplicaciones del ambiente, incluyendo sus reglas, permisos y características de seguridad basado en puertos y protocolos - Debe tener protocolos de monitoreo SNMP v2 y v3. - Debe permitir la administración mediante al menos: línea de comando, interface web gui, ssh v2. - Deberá tener mecanismos que permitan el diagnóstico y telemetría que monitoreen al menos objetos como tenants o inquilinos, perfiles de aplicación y switches. - Deberá permitir la comunicación basada en un modelo de listas blancas, es decir que nada en ella se comunique entre sí a menos que se defina el flujo de comunicación de manera explícita entre los distintos elementos de red, o

	aplicaciones.

ITEM 10: CONTROLADORA INALÁMBRICA DE ACCESS POINTS

Equipo: CONTROLADORA DE ACCESS POINTS	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	Equipo con control centralizado para administración de Access Point
Licenciamiento	Se debe incluir el licenciamiento para el registro de al menos 175 Access Points
Compatibilidad	El equipo propuesto y todas sus funcionalidades deben ser compatibles con el sistema de seguridad de control de acceso ofertado. Indicado en el ítem 11.
Especificaciones generales mínimas	El equipo propuesto debe contar con, al menos, las tecnologías de siguiente generación que se listan a continuación: Inalámbrico: • IEEE 802.11a, 802.11b, 802.11g, WMM / 802.11e, 802.11n , 802.11k, , 802.11u, 802.11ac Substituir por:
	Cableado/Conmutación/Enrutamiento: • Especificación 1000BASE-T, etiquetado IEEE 802.1Q VLAN, agregación de enlaces IEEE 802.1ad Link Aggregation Control Protocol.
	Solicitud de datos para comentarios (RFC) • RFC 768 UDP • RFC 791 IP • RFC 2460 IPv6 • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 2131 DHCP • Mecanismos de auto descubrimiento de APs
	Estándares de seguridad • Acceso protegido Wi-Fi (WPA) • IEEE 802.11i (WPA2, RSN) • RFC 1321 MD5 Message-Digest Algorithm • RFC 1851 ESP Triple DES Transform • RFC 2246 TLS Protocol Version 1.0 • RFC 2409 IKE • Algoritmos de cifrado RFC 2451 ESP CBC-Mode • Certificado Internet X.509
	Cifrado: • Privacidad equivalente por cable (WEP) y protocolo de integridad de clave temporal: comprobación de integridad de mensaje (TKIP-MIC) • Contador con código de cifrado Protocolo de cifrado de mensaje de encadenamiento (CCMP) • Secure Sockets Layer (SSL) y Transport Layer Security (TLS): RC4 de 128 bits y RSA de 1024 y 2048 bits.
	Autenticación, autorización y contabilidad (AAA): • IEEE 802.1X • Autenticación RADIUS RFC 2865 • RFC 2866 RADIUS Contabilidad • Extensiones RFC 2869 RADIUS • RFC 3748 Protocolo de autenticación extensible (EAP) • Autenticación basada en la web • Soporte de TACACS para usuarios de administración
	Administración: • Protocolo simple de administración de redes (SNMP) v1, v2c, v3 • RFC 3164 Syslog • RFC 3418 MIB para SNMP

	Interfaces de Gestión: • Basado en la web: HTTP • Interfaz de línea de comandos: Telnet, protocolo Secure Shell (SSH), puerto serial
	Interfaces e Indicadores: • Al menos 2 x 10Gbps • Al menos 1 puerto de consola: puerto serial (RJ-45) • Indicadores LED: enlace de red, diagnóstico
	Dimensiones Físicas • Al menos 1 (una) UR (Unidad de Rack)
Funcionalidades	SD-Access Wireless: El equipo propuesto debe permitir: - la automatización basada en políticas para el aprovisionamiento automatizado de redes cableadas e inalámbricas, - políticas basadas en grupos para usuarios y dispositivos conectados, - un plano de datos inalámbrico distribuido para implementaciones de campus.
	Analítica y Assurance: El equipo propuesto debe ofrecer visibilidad de red, incluyendo usuarios y dispositivos
	Escalabilidad y rendimiento: El equipo propuesto debe habilitar las redes Wave 2, que admiten: • rendimiento de al menos 20 Gbps • Al menos 1000 puntos de acceso • Al menos 10,000 clientes • Al menos 3900 VLAN
	Gestión de RF: • El equipo propuesto debe identificar la interferencia de señal. • El equipo propuesto debe proporcionar información en tiempo real e histórica de la interferencia de RF que afecta el rendimiento de la red
	Seguridad completa de extremo a extremo: • El equipo propuesto debe ofrecer encriptación y aprovisionamiento de Puntos de Acceso Inalámbricos, encriptación entre los sitios de la WAN y la controladora inalámbrica • El equipo propuesto debe detectar puntos de acceso no autorizados y detección de ataques de denegación de servicio.
	Tolerancia a fallas y alta disponibilidad: • El equipo propuesto debe tener conectividad redundante de al menos 1 Gbps • Debe estar configurado en alta disponibilidad activo–activo ó activo-standby • El equipo propuesto debe disponer de al menos una fuente de poder

ITEM 11: SISTEMA DE CONTROL DE ACCESO A LA RED AAA

Equipo: SISTEMA DE CONTROL DE ACCESO A LA RED	
DESCRIPCIÓN GENERAL	
Tipo de Equipo	El equipo propuesto debe ser centralizado para la seguridad de acceso a la red. Puede ser virtual appliance con las características recomendadas por el fabricante. En caso de ofrecer Virtual Appliance se debe incluir los servidores físicos necesarios para realizar la instalación y disponer de Alta Disponibilidad con la recomendación dada por el fabricante de la solución.
Licenciamiento	Se debe incluir el licenciamiento para al menos 17.000 cuentas base o su equivalente, y 3.000 plus o su equivalente
Especificaciones generales mínimas	Debe soportar al menos la siguiente cantidad de endpoints: • Endpoints Soportados en el Nodo de Política de Servicios: al menos 17.000

	Gestión Centralizada: • El equipo propuesto debe permitir a los administradores configurar y gestionar centralmente los servicios de perfiles, posturas, invitados, autenticación y autorización en una única consola de GUI basada en la web.
	Identidad Contextual y Aplicación de Políticas: • El equipo propuesto debe permitir revisar atributos de al menos el usuario, la identidad del punto final, la validación de la postura, los protocolos de autenticación, la identidad del perfil. • El equipo propuesto debe integrarse con múltiples repositorios de identidad externos como Microsoft Active Directory, Protocolo ligero de acceso a directorios (LDAP) y RADIUS.
	Control de Acceso: • El equipo propuesto debe ofrecer una variedad de opciones de control de acceso, incluidas al menos las listas de control de acceso (DACL) descargables, asignaciones de LAN virtual (VLAN), redirecciones de URL para el portal cautivo y ACL nombradas.
	Gestión del ciclo de vida de los invitados: • El equipo propuesto debe proporcionar flujos visuales en tiempo real del diseño del flujo de invitados • El equipo propuesto debe registrar el acceso a través de la red para seguridad, cumplimiento y auditoría completa de invitados. Debe incluir al menos los límites de tiempo, vencimiento de cuentas.
	Simplificación de dispositivos incorporados: • El equipo propuesto debe permitir a los usuarios finales agregar y administrar sus dispositivos con portales de autoservicio, • El equipo propuesto debe permitir portales cautivos o de sponsor
	Servicios incorporados de AAA: • El equipo propuesto debe utilizar el protocolo RADIUS estándar para Autenticación, Autorización y Contabilidad (AAA). • El equipo propuesto debe admitir al menos los siguientes protocolos de autenticación MS-CHAP, Protocolo de autenticación extensible (EAP) -MD5, EAP protegido (PEAP),y EAP-Transport Layer Security (TLS).
	Control de acceso y auditoría de administración de dispositivos: • El equipo propuesto debe admitir el protocolo TACACS + • El equipo propuesto debe otorgar acceso a los usuarios en función de credenciales, grupos, ubicaciones y comandos. • El equipo propuesto debe mantener registros de auditoría para cada cambio en la red.
	Perfiles de dispositivos: • El equipo propuesto debe permitir crear plantillas de dispositivos predefinidos para al menos 3 equipos (ej, teléfonos IP, impresoras, smartphones, entre otros). • El equipo propuesto debe asociar políticas de autorización específicas de punto final basadas en el tipo de dispositivo.

	Servicio de postura de punto final:
	• El equipo propuesto debe realizar evaluaciones de postura a los puntos finales conectados a la red.
	• El equipo propuesto debe permitir crear políticas que incluyan al menos: verificaciones de los últimos parches del SO, administración de parches.
	• El equipo propuesto debe disponer de un agente para la evaluación de la postura en las plataformas con al menos los siguientes sistemas operativos:
	  o Windows 10, 8.1, 8 y 7
	  o Mac OS X 10.8 y posterior

	Soporte de Active Directory: • El equipo propuesto debe proporcionar autenticación y autorización integrales contra dominios multiformato Microsoft Active Directory. • El equipo propuesto debe agrupar dominios múltiples en grupos lógicos • El equipo propuesto debe incluir reglas de reescritura de identidad flexibles. • El equipo propuesto debe admitir al menos Microsoft Active Directory 2008, 2008R2, 2012, 2012R2 y 2016.
MONITOREO	Monitorización y solución de problemas: • El equipo propuesto debe permitir obtener informes históricos y en tiempo real. • El equipo propuesto debe registrar las actividades de todos los usuarios y puntos finales que se conectan a la red a través de este equipo.

ITEM 12: RACKS

Equipo: RACKS	
DESCRIPCIÓN GENERAL	
Características Generales	• Se deben incluir las PDUs para los racks. • Los Rack serán de al menos 40 RU. • Deben tener estabilizadores y sistema de aterrizaje a tierra • Deben cumplir al menos los estándares industriales: EIAY, certificación UL/CSA. • Deben ser totalmente cerrados, con tapas laterales sólidas y puertas perforadas aseguradas con llave en la parte frontal y posterior; dichas puertas deberán ser de rápida remoción. Debe incluir un panel de bloqueo estándar de la industria en las puertas frontal y posterior.

Enmienda 2:

Parte II. Sección VII. Requisitos de Bienes y Servicios, Servicios Conexos:

Donde dice:

INSTALACIÓN

- *La entrega e instalación del equipamiento adquirido deberá ser entregado de acuerdo a la siguiente distribución:*

Item 1: SWITCH DE ACCESO DE CAPA TRES DE 48 PUERTOS PARA AGENCIAS

...

Item 13: RACKS

	Lugar	***Ciudad***	***Dirección***
	Quito – Centro de Computo	*Quito*	*Paez y Ramirez Davalos*

Debe decir:

INSTALACIÓN

- *La entrega e instalación del equipamiento adquirido deberá ser entregado de acuerdo a la siguiente distribución:*

Item 1: SWITCH DE ACCESO DE CAPA TRES DE 48 PUERTOS

No.	Lugar	Ciudad	Dirección
1	Guayaquil - Mogul	Guayaquil	Av. Juan Tanca Marengo, Km 31/2 Sector 66 Manzana 118 Solar 6
2	Quito – Salinas	Quito	Salinas y Santiago
3	Quito – Salinas	Quito	Salinas y Santiago
4	Quito – Salinas	Quito	Salinas y Santiago
5	Quito – Salinas	Guayaquil	Edif. World Trade Center Av. Francisco de Orellana y Justino Cornejo
6	Quito – Salinas	Quito	Salinas y Santiago
7	Machala	Machala	Av. 25 de Junio Km. 1.5 Vía a Pasaje
8	Machala	Machala	Av. 25 de Junio Km. 1.5 Vía a Pasaje
9	Machala	Machala	Av. 25 de Junio Km. 1.5 Vía a Pasaje
10	Riobamba	Riobamba	Primera Constituyente s/n y Espejo (esq.)
11	Riobamba	Riobamba	Primera Constituyente s/n y Espejo (esq.)
12	Portoviejo	Portoviejo	Calle Olmedo entre Sucre y Córdova, Oficinas del Edificio Ex-Previsora
13	Portoviejo	Portoviejo	Calle Olmedo entre Sucre y Córdova, Oficinas del Edificio Ex-Previsora
14	Portoviejo	Portoviejo	Calle Olmedo entre Sucre y Córdova, Oficinas del Edificio Ex-Previsora
15	Portoviejo	Portoviejo	Calle Olmedo entre Sucre y Córdova, Oficinas del Edificio Ex-Previsora
16	Loja	Loja	Bernardo Valdivieso 08–54 entre Rocafuerte y 10 de Agosto
17	Loja	Loja	Bernardo Valdivieso 08–54 entre Rocafuerte y 10 de Agosto
18	Loja	Loja	Bernardo Valdivieso 08–54 entre Rocafuerte y 10 de Agosto
19	Ambato	Ambato	Juan Montalvo S/N y Av. 12 de Noviembre
20	Ambato	Ambato	Juan Montalvo S/N y Av. 12 de Noviembre
21	Ambato	Ambato	Juan Montalvo S/N y Av. 12 de Noviembre
22	Cuenca	Cuenca	Av. Remigio Crespo 5–28 y Lorenzo Piedra
23	Cuenca	Cuenca	Av. Remigio Crespo 5–28 y Lorenzo Piedra
24	Santa Cruz	Santa Cruz	Puerto Ayora, Av. Baltra s/n y San Cristóbal
25	Cuenca	Cuenca	Av. Remigio Crespo 5–28 y Lorenzo Piedra
26	Cuenca	Cuenca	Av. Remigio Crespo 5–28 y Lorenzo Piedra
27	Cuenca	Cuenca	Av. Remigio Crespo 5–28 y Lorenzo Piedra
28	Cuenca	Cuenca	Av. Remigio Crespo 5–28 y Lorenzo Piedra
29	Machala	Machala	Av. 25 de Junio Km. 1.5 Vía a Pasaje
30	Riobamba	Riobamba	Primera Constituyente s/n y Espejo (esq.)
31	Portoviejo	Portoviejo	Calle Olmedo entre Sucre y Córdova, Oficinas del Edificio Ex-Previsora
32	Loja	Loja	Bernardo Valdivieso 08–54 entre Rocafuerte y 10 de Agosto
33	Ambato	Ambato	Juan Montalvo S/N y Av. 12 de Noviembre
34	Cuenca	Cuenca	Av. Remigio Crespo 5–28 y Lorenzo Piedra
35	Quito – Salinas	Quito - Salinas	Salinas y Santiago
36	Quito - Salinas	Quito - Salinas	Salinas y Santiago
37	Latacunga	Latacunga	Sánchez de Orellana y Padre Salcedo 15–68
38	Guaranda	Guaranda	7 de Mayo s/n y García Moreno (esq.)

No.	Lugar	Ciudad	Dirección
39	Puyo	Puyo	Ceslao Marín y Av. Curaray Esq. frente al Hospital del IESS
40	Orellana	Orellana	Av. 9 de Octubre y Jorge Rodríguez (esquina)
41	Azogues	Azogues	Serrano 7-14 entre Matovelle y Malo
42	Santo Domingo	Santo Domingo	Av. Quito No. 1486 y Calle Los Naranjos
43	Santo Domingo	Santo Domingo	Av. Quito No. 1486 y Calle Los Naranjos

Item 2: ACCESS POINTS

No.	Lugar	Ciudad	Dirección
1	Quito - Salinas	Quito	Salinas y Santiago
2	Quito - Salinas	Quito	Salinas y Santiago
3	Quito - Salinas	Quito	Salinas y Santiago
4	Quito - Salinas	Quito	Salinas y Santiago
5	Cuenca	Cuenca	Av. Remigio Crespo 5-28 y Lorenzo Piedra
6	Portoviejo	Portoviejo	Calle Olmedo entre Sucre y Córdova, Oficinas del Edificio Ex-Previsora
7	Guayaquil - WTC	Guayaquil	Edif. World Trade Center Av. Francisco de Orellana y Justino Cornejo
8	Quito - Amazonas	Quito	Amazonas y Roca
9	Cuenca	Cuenca	Av. Remigio Crespo 5-28 y Lorenzo Piedra
10	Guayaquil - WTC	Guayaquil	Edif. World Trade Center Av. Francisco de Orellana y Justino Cornejo
11	Quito - Agencia Amazonas	Quito	García Moreno 769 y Sucre
12	Guayaquil - WTC	Guayaquil	Edif. World Trade Center Av. Francisco de Orellana y Justino Cornejo
13	Cuenca	Cuenca	Av. Remigio Crespo 5-28 y Lorenzo Piedra
14	Quito - Salinas	Quito	Salinas y Santiago

Item 3: ROUTER CONCENTRADOR DE ENLACES ENTIDADES EXTERNAS

No.	Lugar	Ciudad	Dirección
1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Item 4: CONTROLADORA PARA MONITOREO Y GESTION PARA SWITCHES Y ACCESS POINTS

No.	Lugar	Ciudad	Dirección
1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Item 5: SWITCH LEAF DE 48 PUERTOS MÍNIMO 10Gbps

No.	Lugar	Ciudad	Dirección
1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Item 6: SWITCH LEAF DE 32 PUERTOS MÍNIMO A 40Gbps

No.	Lugar	Ciudad	Dirección

1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Item 7: SWITCH LEAF DE 48 PUERTOS MINIMO A 10/25 Gbps

No.	Lugar	Ciudad	Dirección
1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Item 8: SWITCH SPINE DE 64 PUERTOS MÍNIMO A 40/100 Gbps

No.	Lugar	Ciudad	Dirección
1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Item 9: CONTROLADORA DE DATA CENTER EN CLUSTER PARA SWITCH SPINE AND LEAF

No.	Lugar	Ciudad	Dirección
1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Item 10: CONTROLADORA INALÁMBRICA DE ACCESS POINTS

No.	Lugar	Ciudad	Dirección
1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Item 11: SISTEMA DE CONTROL DE ACCESO A LA RED AAA

No.	Lugar	Ciudad	Dirección
1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Item 12: RACKS

No.	Lugar	Ciudad	Dirección
1	Quito – Centro de Computo	Quito	Páez y Ramírez Dávalos

Enmienda 3:

Parte II. Sección VII. Requisitos de Bienes y Servicios, Servicios Conexos , Garantía Técnica, cuarta viñeta (Página 203):

Donde dice:

> *"Para los equipos descritos en las especificaciones técnicas, bienes requeridos; ítems 3 al 13, la asistencia será 24x7; es decir soporte 24 horas al día, durante los 7 días de la semana, y una respuesta de máximo 2 horas luego de reportado el incidente, para resolución de problemas críticos de los equipos conforme se indica en el apartado de garantía técnica."* .

Debe decir:

> *"Para los equipos descritos en las especificaciones técnicas, bienes requeridos; ítems 3 al 12 (modificado mediante boletín de enmiendas No. 2), la asistencia será 24x7; es decir soporte*

24 horas al día, durante los 7 días de la semana, y una respuesta de máximo 2 horas luego de reportado el incidente, para resolución de problemas críticos."

Enmienda 4:

Parte II. Sección VII, Requisitos de Bienes y Servicios, Servicios Conexos , Garantía Técnica, quinta viñeta (Página 203):

Donde dice:

"Para los equipos descritos en las especificaciones técnicas, infraestructura actual, tabla 5 (Cisco Prime y MSE), o la consola de gestión centralizada propuesta la asistencia 24x7; es decir soporte 24 horas, durante los 7 días de la semana, y una respuesta de máximo 2 horas laborables luego de reportado el incidente, para resolución de problemas críticos de los equipos conforme se indica en el apartado de garantía técnica" .

Debe decir:

"En caso de que la solución propuesta requiera utilizar el CISCO PRIME Y MSE detallados en la tabla 5 bajo el título Infraestructura actual, página 168, se deberá renovar la garantía técnica y garantizar la asistencia 24x7; es decir, soporte 24 horas, durante los 7 días de la semana, y una respuesta de máxima 2 horas luego de reportado el incidente, para la resolución de problemas críticos" .

Enmienda 5:

Parte I. Sección IV, Formularios de la Oferta, páginas 53 a 145.

Se reemplaza íntegramente el Formulario de Cumplimiento de Especificaciones Técnicas, por el que se encuentra adjunto.

Enmienda 6:

El cronograma del proceso modificado es el siguiente:

Publicación de boletines Nos. 2	24 de julio de 2019
Plazo adicional para preguntas	29 de julio de 2019
Plazo para presentación de ofertas	13 de agosto de 2019, 10h00.
Apertura de ofertas	13 de agosto de 2019, 11h00

Quito, 24 de julio de 2019