CONVENIO MARCO MJ Y DH CAMARA DEL COMERCIO AUTOMOTOR- CCA
LEY 23.283 23.412

Ciudad Autónoma de Buenos Aires, 28 de Enero del 2026

NOTA ACLARATORIA

ASUNTO: CONCURSO PRIVADO DE PRECIOS ADQUISICIÓN DE EQUIPAMIENTO WIFI Y DE RED PARA EDIFICOS SARMIENTO 329 Y COCHABAMBA 54, CABA

Estimados:

Por la presente, adjuntamos invitación para Concurso Privado de Precios.

A tal efecto, informamos que las ofertas se recibirán hasta **el día 10 de Febrero a las 12 hs.**

Por e-mail en la casilla de correo: melina@cca.org.ar

Sin otro particular, saluda atentamente.

Fernando La Iglesia
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412

Ricardo Orsi
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412

SOLER 3909 - (1425) CABA TEL. 4824-7272 / 9505 / 9498 / 9489 FAX. 4822-7453 4823-1837

CONVENIO MARCO MJ Y DH CAMARA DEL COMERCIO AUTOMOTOR- CCA
LEY 23.283 23.412

Ciudad Autónoma de Buenos Aires, 28 de Enero del 2026

Señores

PROVEEDORES

Presente

Concurso Privado de Precios Adquisición de equipamiento Wifi y de Red para edificios Sarmiento 329 y Cochabamba 54, CABA

EXPEDIENTE: ALC—235/2026

De nuestra mayor consideración:

Nos dirigimos a Uds. a efectos de invitarlos a participar en la presentación de ofertas para la adquisición del siguiente elemento.

ELEMENTOS	**CANTIDAD** (LEER ESPECIFICACIONES TECNICAS)
SWITCHS 24 PUERTOS	12
SWITCHS 48 PUERTOS	12
PUNTO DE ACCESO INALÁMBRICO	130
CONTROLADORA WIFI NUBE	1
CONTROLADORA WIFI NAC	1

CONVENIO MARCO MJ Y DH CAMARA DEL COMERCIO AUTOMOTOR- CCA
LEY 23.283 23.412

Fecha Presentación de la Oferta: 10 de Febrero del año 2026.

Hora: 12 hs.

Las ofertas deben presentarse con la documentación debidamente firmada, indicando en forma destacada nombre de la firma oferente y fecha del Concurso a realizarse.

Validez de presupuestos: 30 días

Precio: deben indicar el valor total con IVA INCLUIDO.

Firma, Aclaración, Teléfono, Mail, Domicilio, Cuit.

-Mantenimiento de la Oferta: 30 (treinta) días corridos a partir del día de apertura de sobres, renovables automáticamente salvo aviso en contrario con 10 (diez) días de anticipación.

Documentación a Presentar en el Acto de Apertura:

.- **Garantía de Oferta:** Pagaré simple por el 5 % del importe total de la oferta, suscripto por el Apoderado si supera el millón de pesos.

.- **Aceptación de Condiciones:** Se deberá adjuntar a la oferta, la presente invitación firmada por el apoderado de la compañía en todas sus hojas, aceptando las condiciones establecidas en la presente.

Adjudicación: Se adjudicará por renglón al oferente que presente menor precio y cumpla con las especificaciones técnicas. Según conformidad del Ministerio de Justicia y Derechos Humanos.

Forma de Pago: Contra entrega.

CONVENIO MARCO MJ Y DH CAMARA DEL COMERCIO AUTOMOTOR- CCA
LEY 23.283 23.412

Enviar la documentación a las siguientes casillas de correo: melina@cca.org.ar

Sin más, saludamos Atte.

Fernando La Iglesia
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412

Ricardo Orsi
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412

SOLER 3909 - (1425) BUENOS AIRES TEL. 4824-7272 / 9505 / 9498 / 9489 FAX. 822-7453 823-1837

MINISTERIO DE JUSTICIA

PLIEGO DE ESPECIFICACIONES TÉCNICAS

EQUIPAMIENTO WIFI Y DE RED PARA EDIFICIOS DEL MINISTERIO DE JUSTICIA

1. OBJETO:

La presente contratación tiene por objeto la provisión de equipamiento WIFI y de Red para los edificios del MINISTERIO DE JUSTICIA sitos en Sarmiento N° 329 y Cochabamba N° 54 de la CIUDAD AUTÓNOMA DE BUENOS AIRES.

2. DETALLES DE LA CONTRATACIÓN:

La contratación objeto de las presentes especificaciones técnicas deberá ser una solución para garantizar la continuidad operativa y la protección de los activos digitales del MINISTERIO DE JUSTICIA, consistente en los siguientes pilares:

a. ***Conectividad de acceso: Implementación de una capa de switching robusta con el sistema operativo, diseñada para soportar las demandas actuales de PoE y tráfico de alta velocidad con latencias mínimas.***

b. ***Movilidad de nueva generación: Despliegue de tecnología Wi-Fi 7, asegurando una infraestructura preparada para el futuro con soporte en la banda de 6 GHz y capacidades de localización IoT integradas.***

c. ***Gestión inteligente: Orquestación centralizada en la nube que permite una administración simplificada, visibilidad total del tráfico mediante IA (AIOps) y soporte técnico proactivo 24x7 por suscripción.***

d. ***Control de Acceso Seguro a la red: Una arquitectura de seguridad "Zero Trust" que garantiza que el acceso a los***

recursos de la red sólo se otorgue a los usuarios y dispositivos autorizados, que cumplan con las políticas de seguridad exigidas.

3. ***CONDICIONES GENERALES:***

Al ser un ecosistema integrado toda la solución deberá ser del mismo fabricante, para ello el oferente deberá presentar una nota suscripta por el fabricante que lo habilite a presentar la propuesta en el presente concurso de precios.

4. ***RENGLONES INVOLUCRADOS:***

RENGLÓN	DETALLE	CANTIDAD
1	SWITCHS 24 PUERTOS	12
2	SWITCHS 48 PUERTOS	12
3	PUNTO DE ACCESO INALÁMBRICO	130
4	CONTROLADORA WIFI NUBE	1
5	CONTROLADORA WIFI NAC	1

A continuación se detalla la totalidad de los renglones que conforman la presente contratación:

5. ***REQUISITOS TÉCNICOS DE LA SOLUCIÓN:***

    a. ***RENGLÓN 1: SWITCH DE ACCESO 24 PUERTOS:***

Cantidad: DOCE (12)

Detalle: Los equipos deben proporcionarse con kit de rackeo correspondiente y suscripción a CINCO (5) años.

Características técnicas: El switch deberá cumplir con las características técnicas que se enuncian a continuación.

- ***arquitectura: Switch Acceso, L2/L3***
- ***puertos para datos:***
    - ***24x puertos 10/100/1000BASE-T Clase 4 PoE , soportar hasta 30W por puerto***
    - ***. 4x puertos 1/10G SFP***
    - ***Soportar estándares PoE IEEE 802.3af, 802.3at***
    - ***Todas las interfaces deben estar habilitadas, activas y listas para su uso. El proveedor deberá incluir todo el licenciamiento que el equipo requiera para cumplir esta condición.***
- ***puertos para administración***
    - ***1 puerto consola USB-C***
    - ***1 USB para administración de archivos.:***
- ***características de memoria: 4 GB DDR3, 16 GB eMMC flash; packet buffer : 1 MB***
- ***rendimiento: Arquitectura nonblocking, Switching 128 Gbps, Throughput 95.2 Mpps,***
- ***apilamiento:***

- ***Capacidad de conectarse en stack con otro switch de la misma familia de switches de manera física.***
- ***Los equipos que son parte del cluster o stack deberán comportarse como un dispositivo virtual.***
- ***El cluster o stack debe ser capaz de crecer al menos hasta seis (6) equipos (con otros de 24/48 puertos de la misma familia)***
- ***Proveer todo el hardware y software necesario para conectar los equipos mediante al menos dos (2) enlaces de 10GE.***

- ***Sistema operativo: El sistema operativo debe incluir el licenciamiento de todos los puertos y características de servicio que el equipo pueda soportar.***
- ***Requerimientos L2***
  - ***tamaño de tablas:- 8192 direcciones MAC***
  - ***VLANs: - 4094 VLAN Ids (512 simultáneas)***
  - ***Tramas: - Jumbo frames de 9220 bytes***
  - ***Spanning tree***
    - ***Spanning tree estándar IEEE 802.1D***
    - ***Rapid STP IEEE 802.1w***
    - ***Multiple STP (MSTP) IEEE 802.1s***
    - ***Rapid Per-VLAN Spanning Tree (RPVST+)***
  - ***Características***
    - ***MVRP aprendizaje automático y asignación dinámica de VLANs***
    - ***IGMP para el manejo y control de multicast en capa 2***
    - ***IEEE 802.3ad LACP, soporte de 8 grupos (cada grupo con soporte de hasta 8 enlaces), grupos dinámicos o estáticos***

y selección del algoritmo de hashing

- *LLDP-MED*
- *Configuración automática de VLAN para teléfonos IP*

- *requerimientos L3*
  - *performance*
    - *1024 entradas IPv4*
    - *512 entradas IPv6*
    - *1024 entradas ARP*
    - *512 Rutas unicast IPv4/IPv6*
    - *16 SVI*
    - *256 entradas ACL IPv4*
    - *128 entradas ACL IPv6*
    - *256 entradas ACL MAC*
  - *protocolos*
    - *Rutas estáticas IPv4/IPv6*
    - *Dual Stack IPv4/IPv6*
  - *características*
    - *ARP: estático, gratuitous*
    - *DNS: cliente*
    - *DHCP: relay, cliente*
- *Multicast*
  - *Multicast Listener Discovery*
    - *MLD v1 y v2*

        - ***MLD para IPv6***
    - ***Protocol Independent Multicast (PIM): IGMP Snooping***
    - ***Internet Group Management (IGMP): IGMP v1, v2 y v3***
- ***Qos***
    - ***Encolamiento: Al menos Strict Priority.***
    - ***Servicio: Al menos:***
        - ***802.1p***
        - ***QOS trust COS - DSCP***
        - ***CoS utlizando dirección IP, Type of service, protocolo capa 3, puerto UDP/TCP, diffserv***
- ***Seguridad:***
    - ***Autenticación para administración. Soporte de:***
        - ***Radius***
        - ***TACACS+***
    - ***Autenticación de usuarios: Soporte de:-***
        - ***Autenticación por dirección MAC***
        - ***Radius***
        - ***802.1x***
        - ***Autenticación basada en WEB desde un portal cautivo externo.***
        - ***Autenticación concurrente de los esquemas de autenticación IEEE 802.1X, web y MAC por puerto.***
        - ***Radius CoA***
    - ***Políticas basadas en roles: Integración con Sistema de Control de Acceso AAA para asignar políticas basada en el rol del***

usuario que se conecta, como ACL y VLAN.

- ***Gestión segura: Acceso seguro a la gestión cifrando el tráfico (CLI, GUI, MIB) por medio de SSHv2, SSL, SNMPv3. Al menos:***
  - ***Listas de acceso de control (ACL) soportadas en IPv4 e IPv6, para controlar el acceso no autorizado a la red y para controlar el tráfico. Las reglas niegan o permiten el tráfico y se pueden basar en los headers de capa 2 o capa 3. También proporcionan filtrado basado en los campos IP, subredes e IPs origen/destino, puertos TCP/UDP origen/destino sobre VLANs o puertos.***
  - ***Protección de CPU ante tráfico malicioso que intente interrumpir el servicio del equipo***
  - ***Limitación de tráfico ICMP de negación de servicio***
  - ***Protección de BPDU STP en puertos que no se requiera este protocolo***
  - ***Protección de STP root de ataques maliciosos o por errores de configuración***
  - ***Protección dinámica de ARP para el bloqueo de ARP desde host no autorizados, evitando escuchas o robo de datos de la red.***
  - ***Port security permite el acceso de direcciones MAC específicas, que pueden ser aprendidas o especificadas por el administrador***
  - ***MAC address lockout evita que direcciones MAC configuradas específicas se conecten a la red.***
  - ***Despliegue de banner de seguridad***
  - ***RadSec para utilización del protocolo RADIUS de forma segura***
  - ***Private VLAN (PVLAN)***

- ***Bloqueo dinámico de IP para bloquear el tráfico de hosts no autorizados y evitar la suplantación de direcciones IP de origen***
- ***Rol de autenticación crítico que garantiza que los dispositivos de infraestructura importantes, como los teléfonos IP, tengan acceso a la red incluso en ausencia de un servidor RADIUS.***
- ***TPM (Trusted Platform Module) para asegurar la integridad de la plataforma***
- ***DHCP Snooping protección ante oferta de DHCP de host no autorizados***

- ***Control de tormentas: Protección contra tormentas de datos broadcast, multicast y unicast con umbrales definidos por el cliente.***
- ***alta disponibilidad: Al menos:***
  - ***Soporte de UDLD (Uni-directional Link Detection) para monitorear la conectividad del enlace y apagar puertos en ambos extremos si se detecta tráfico unidireccional, evitando loops en redes basadas en STP***
  - ***Proporcionar imágenes flash duales de archivos independientes del sistema operativo primario y secundario.***

- ***Gestión***
  - ***administración***
    - ***Capacidad de administración CLI, GUI (embebidas), o Nube mediante esquema de subscripcion.***
    - ***CLI estándar de industria con una estructura jerárquica para reducir el tiempo y los gastos de capacitación. Ofrece mayor productividad en entornos de múltiples***

proveedores

- ***Interfaz API REST integrada, programable y fácil de usar***
- ***Aprovisionamiento de día cero***
- ***sFlow (RFC 3176)***
- ***Restricción en comandos para configuraciones críticas, proporcionar múltiples niveles de privilegios con protección por contraseña, registro de acceso local y remoto por syslog.***
- ***TACACS+ proporciona autorización de acceso administrativo***
- ***SNMP (v2c/v3) , MIBs estándar y extensiones privadas***
- ***RMON***
- ***TFTP, SFTP, SSH***
- ***NTP***
- ***Almacenamiento de múltiples archivos de configuración en memoria flash***
- ***Port mirroring para tráfico saliente y entrante; soportar hasta 4 grupos de mirror***

- ***Hardware y energía***
  - ***montaje: Debe traer todos los accesorios para montaje y operación en rack estándar de 19"***
  - ***alimentación eléctrica: Soporte al menos:***
    - ***100V–127V/200V–240V***
    - ***50 Hz/60 Hz.***
    - ***Ventilador interno***
  - ***Redundancia en fuente de poder: 1 fuente interna. Mínima***

potencia PoE 370W

- ***Redundancia en ventilación: Ventilador interno***
- ***Medio ambiente: cumplir al menos:***
  - ***RoHS***
  - ***WEEE***
  - ***Soporte de IEEE 802.3az***
- ***temperatura de operación: 0°C a 45°C hasta 5000 pies; reducir 1 °C por cada 1000 pies desde 5000 pies a 10 000 pies.***
- ***Humedad de operación: 15% a 95% a 40°C no condensada***

- ***Garantía y soporte:***
  - ***Garantía limitada de por vida***
    - ***Duración de garantía EOS + CINCO (5) años***
    - ***Vida útil limitada: la cobertura de la garantía se amplía sólo durante el tiempo que el usuario final original de buena fe posea o haga uso del producto***

b. RENGLÓN 2: SWITCH DE ACCESO 48 PUERTOS:

Cantidad: DOCE (12)

Detalle: Los equipos deben proporcionarse con kit de rackeo correspondiente y suscripción a CINCO (5) años.

Características técnicas: El switch deberá cumplir con las características técnicas que se enuncian a continuación.

- ***arquitectura: Switch Acceso, L2/L3***
- ***interfaces:***
  - ***puertos para datos:***
    - ***48x puertos 10/100/1000BASE-T Clase 4 PoE , soportar hasta 30W por puerto***

        - ***4x puertos 1G/10G SFP***
        - ***Soportar estándares PoE IEEE 802.3af, 802.3at***
        - ***Todas las interfaces deben estar habilitadas, activas y listas para su uso. El proveedor deberá incluir todo el licenciamiento que el equipo requiera para cumplir esta condición.***
    - ***puertos para administración:***
        - ***1 puerto consola USB-C***
        - ***1 USB para administración de archivos.***
- ***características generales y performance***
    - ***Características de memoria: 4 GB DDR3, 16 GB eMMC flash; packet buffer : 1 MB***
    - ***Rendimiento:***
        - ***Switching 176 Gbps***
        - ***Throughput 98.6 Mpps***
        - ***Arquitectura nonblocking***
    - ***apilamiento:***
        - ***Capacidad de conectarse en stack con otro switch de la misma familia de switches de manera física***
        - ***Los equipos que son parte del cluster o stack deberán comportarse como un dispositivo virtual.***
        - ***El cluster o stack debe ser capaz de crecer al menos hasta seis (6) equipos (con otros de 24/48 puertos de la misma familia)***
        - ***Proveer todo el hardware y software necesario para conectar los equipos mediante al menos dos (2) enlaces de 10GE.***

- ***Sistema operativo:***
  - ***El sistema operativo debe incluir el licenciamiento de todos los puertos y características de servicio que el equipo pueda soportar.***

- ***Requerimiento L2***
  - ***tamaño de tablas: 8192 direcciones MAC***
  - ***VLANS: 4094 VLAN Ids (512 simultaneas)***
  - ***tramas: Jumbo frames de 9220 bytes***
  - ***Spanning tree:***
    - ***Spanning tree estándar IEEE 802.1D***
    - ***Rapid STP IEEE 802.1w***
    - ***Multiple STP (MSTP) IEEE 802.1s***
    - ***Rapid Per-VLAN Spanning Tree (RPVST+)***
  - ***características:***
    - ***MVRP aprendizaje automático y asignación dinámica de VLANs***
    - ***IGMP para el manejo y control de multicast en capa 2***
    - ***IEEE 802.3ad LACP, soporte de 8 grupos (cada grupo con soporte de hasta 8 enlaces), grupos dinámicos o estáticos y selección del algoritmo de hashing***
    - ***LLDP-MED***
    - ***Configuración automática de VLAN para teléfonos IP***

- ***Requerimientos L3***
  - ***performance:***
    - ***1024 entradas IPv4***

        - ***512 entradas IPv6***
        - ***1024 entradas ARP***
        - ***512 Rutas unicast IPv4/IPv6***
        - ***16 SVI***
        - ***256 entradas ACL IPv4***
        - ***128 entradas ACL IPv6***
        - ***256 entradas ACL MAC***
    - ***protocolos:***
        - ***Rutas estáticas IPv4/IPv6***
        - ***Dual Stack IPv4/IPv6***
    - ***características.***
        - ***ARP: estático, gratuitous***
        - ***DNS: cliente***
        - ***DHCP: relay, cliente***
- ***Multicast:***
    - ***Multicast Listener Discovery:***
        - ***MLD v1 y v2***
        - ***MLD para IPv6***
    - ***Protocol Independent Multicast (PIM): IGMP Snooping***
    - ***Internet Group Management (IGMP): IGMP v1, v2 y v3***
- ***QoS***
    - ***Encolamiento: Al menos Strict Priority***
    - ***Servicio: Al menos:***

        - ***802.1p***
        - ***QOS trust COS - DSCP***
        - ***CoS utlizando dirección IP, Type of service, protocolo capa 3, puerto UDP/TCP, diffserv***

- ***Seguridad***
    - ***Autenticación para administración:***
        - ***Soporte de: Radius y TACACS+***
    - ***Autenticación de usuarios. Soporte de:***
        - ***Autenticación por dirección MAC***
        - ***Radius***
        - ***802.1x***
        - ***Autenticación basada en WEB desde portal cautivo externo.***
        - ***Autenticación concurrente de los esquemas de autenticación IEEE 802.1X, web y MAC por puerto.***
        - ***- Radius CoA***
    - ***Políticas basadas en roles: Integración con Sistema de Control de Acceso AAA para asignar políticas basada en el rol del usuario que se conecta, como ACL y VLAN.***
    - ***Gestión segura: Acceso seguro a la gestión cifrando el tráfico (CLI, GUI, MIB) por medio de SSHv2, SSL, SNMPv3***
    - ***Características. Al menos:***
        - ***Listas de acceso de control (ACL) soportadas en IPv4 e IPv6, para controlar el acceso no autorizado a la red y para controlar el tráfico. Las reglas niegan o permiten el tráfico y se pueden basar en los headers de capa 2 o capa 3. También proporcionan filtrado basado en los campos IP,***

subredes e IPs origen/destino, puertos TCP/UDP origen/destino sobre VLANs o puertos.

- ***Protección de CPU ante tráfico malicioso que intente interrumpir el servicio del equipo***
- ***Limitación de tráfico ICMP de negación de servicio***
- ***Protección de BPDU STP en puertos que no se requiera este protocolo***
- ***Protección de STP root de ataques maliciosos o por errores de configuración***
- ***Protección dinámica de ARP para el bloqueo de ARP desde host no autorizados, evitando escuchas o robo de datos de la red.***
- ***Port security permite el acceso de direcciones MAC específicas, que pueden ser aprendidas o especificadas por el administrador***
- ***MAC address lockout evita que direcciones MAC configuradas específicas se conecten a la red.***
- ***Despliegue de banner de seguridad***
- ***RadSec para utilización del protocolo RADIUS de forma segura***
- ***Private VLAN (PVLAN)***
- ***Bloqueo dinámico de IP para bloquear el tráfico de hosts no autorizados y evitar la suplantación de direcciones IP de origen***
- ***Rol de autenticación crítico que garantiza que los dispositivos de infraestructura importantes, como los teléfonos IP, tengan acceso a la red incluso en ausencia de un servidor RADIUS.***

        - ***TPM (Trusted Platform Module) para asegurar la integridad de la plataforma***
        - ***DHCP Snooping protección ante oferta de DHCP de host no autorizados***
    - ***Control de tormentas: Protección contra tormentas de datos broadcast, multicast y unicast con umbrales definidos por el cliente.***
    - ***Alta disponibilidad. Al menos:***
        - ***Soporte de UDLD (Uni-directional Link Detection) para monitorear la conectividad del enlace y apagar puertos en ambos extremos si se detecta tráfico unidireccional, evitando loops en redes basadas en STP***
        - ***Proporcionar imágenes flash duales de archivos independientes del sistema operativo primario y secundario***
- ***Gestión***
    - ***Administración:***
        - ***Capacidad de administración CLI, GUI (embebidas), o Nube mediante esquema de suscripción.***
        - ***CLI estándar de industria con una estructura jerárquica para reducir el tiempo y los gastos de capacitación. Ofrece mayor productividad en entornos de múltiples proveedores***
        - ***Interfaz API REST integrada, programable y fácil de usar***
        - ***Aprovisionamiento de día cero***
        - ***sFlow (RFC 3176)***
        - ***Restricción en comandos para configuraciones críticas, proporcionar múltiples niveles de privilegios con***

protección por contraseña, registro de acceso local y remoto por syslog.

- ***TACACS+ proporciona autorización de acceso administrativo***
- ***SNMP (v2c/v3) , MIBs estándar y extensiones privadas***
- ***RMON***
- ***TFTP, SFTP, SSH***
- ***NTP***
- ***Almacenamiento de multiples archivos de configuración en memoria flash***
- ***Port mirroring para tráfico saliente y entrante; soportar hasta 4 grupos de mirror***

- ***Hardware y energía:***
  - ***montaje: Debe traer todos los accesorios para montaje y operación en rack estándar de 19"***
  - ***Alimentación eléctrica: Soporte al menos:***
    - ***100V–127V/200V–240V***
    - ***50 Hz/60 Hz.***
    - ***Ventilador interno***
  - ***Redundancia en fuente de poder: 1 fuente interna con al menos 740W potencia PoE***
  - ***Redundancia en ventilación: Ventilador interno***
  - ***Medio ambiente: Cumplir al menos:***
    - ***RoHS***
    - ***WEEE***

- ***Soporte de IEEE 802.3az***

- ***Temperatura de operación: 0°C a 45°C hasta 5000 pies; reducir 1 °C por cada 1000 pies desde 5000 pies a 10 000 pies.***
- ***Humedad de operación: 15% a 95% a 40°C no condensada***

- ***Garantía limitada de por vida:***
  - ***Duración de garantía EOS + CINCO (5) años***
  - ***Vida útil limitada: la cobertura de la garantía se amplía sólo durante el tiempo que el usuario final original de buena fe posea o haga uso del producto***

c. RENGLÓN 3: PUNTO DE ACCESO INALÁMBRICO:

Cantidad: CIENTO TREINTA (130)

Detalle: Los equipos deben proporcionarse con kit de rackeo correspondiente y suscripción a CINCO (5) años

Características técnicas: El punto de acceso inalámbrico deberá cumplir con las características técnicas que se enuncian a continuación.

- ***Requerimiento L3***
  - ***calificación tecnológica: Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para los requerimientos futuros, los equipos de comunicación ofertados deben corresponder a una marca o fabricante que figure como líder en el cuadrante de Cuadrante Mágico Gartner para soluciones de acceso LAN Wired and Wireless durante al menos los últimos cinco años. Debe presentar el informe correspondiente a cada año.***
  - ***Tipo de equipo: Punto de acceso (Access Point, AP) de red inalámbrica para interiores.***

- ***fabricación: El equipo debe ser nuevo, no remanufacturado.***

- ***características específicas:***
  - ***Estándar WiFi: WiFi7 - 802.11be***
  - ***Bandas de operación: 2.4 / 5 / 6 GHz***
  - ***Especificaciones de radio: 2x2 en todos sus radios***
  - ***Concurrencia: Hasta 512 clientes asociados por radios, y hasta 16 BSSIDs por radio***
  - ***Desempeño:***
    - ***2.4GHz - Hasta 688 Mbps***
    - ***5 GHz - Hasta 2.9 Gbps***
    - ***6 GHz - Hasta 5.8 Gbps***
    - ***Hasta 14.4 Gbps de forma agregada***
  - ***Ganancia de las antenas***
    - ***2.4GHz - Al menos 5.1 dBi***
    - ***5 GHz - Al menos 5.5 dBi***
    - ***6 GHz - Al menos 5.3 dBi***
    - ***Antena omnidireccional downtilt***
  - ***interfaces: 2 x 1/2.5/5Gbps Base-T***
  - ***Alta disponibilidad: Las dos interfaces deben estar en la capacidad de configurarse para proporcionar redundancia de datos (soportando LACP) y energía en caso de falla***
  - ***PoE: El equipo debe soportar PoE 802.3at/bt***
  - ***Interfaces adicionales: Debe tener las siguientes interfaces:***
    - ***2 puertos USB 2.0***

        - ***indicadores visuales LED***
        - ***Botón de reinicio***
        - ***Consola serial***
        - ***Slot de seguridad***

- ***Optimización de redes WiFI***
    - ***Manejo de interferencia: Soportar mecanismos para disminuir la interferencia entre los canales de 5GHz y 6 GHz - Ultra Tri Band Filtering***
    - ***Optimización de clientes: Debe soportar tecnologías que eviten Sticky clients, y realizar balanceo de clientes y carga de aps.***
    - ***Gestión de radio: Proporcionar mecanismos para ajustar dinamicamente anchos de banda, canales y potencias, con el objetivo de reducir la interferencia co-canal***
    - ***Coexistencia con redes: Ofrecer mecanismos para minimizar el impacto de la interferencia de redes celulares***
    - ***Ahorro de energía: Capacidad de entrar en un modo de ahorro de energía cuando la demanda sea baja, para soportar iniciativas de sostenibilidad y ofrecer ahorros en el consumo de energía***
    - ***funcionalidades: Deberá soportar las siguientes tecnologías:***
        - ***MRC - Maximum ratio combining***
        - ***CDD/CSD - Cyclic delay/shift diversity***
        - ***STBC - Space-time block coding***
        - ***LDPC - Low-density parity check***
        - ***TWT - Target Wake Time***
        - ***OFDMA - Orthogonal frequency-division multiplexing***

        - ***BSS Coloring***
        - ***MLO - multi-link operation***

- ***Soporte de iniciativas tecnológicas***
    - ***Localización en interiores: El AP debe servir como referencia para habilitar soluciones de localización en interiores, y proporcionar la localización de un cliente a un sistema tercero***
    - ***Localización en interiores:***
        - ***Soportar FTM 802.11mc/az para mejorar la precisión en la ubicación de los clientes, así como tener un receptor GNSS (GPS)***
        - ***Soportar sensor barométrico para determinar la altitud relativa del AP***
    - ***IoT: El AP debe incluir radios ZigBee y Bluetooth para el soporte de iniciativas de transformación digital***
- ***Seguridad:***
    - ***Autenticación: Soportar WPA3 y Enhanced Open para ofrecer un cifrado robusto***
    - ***Cifrado: Soporte de MACsec***
    - ***Módulos: Incluir módulos de cifrado para asegurar las credenciales, llaves y códigos de booteo***
    - ***Autenticación de usuarios: Soportar integración con soluciones de NAC para simplificar el acceso de los usuarios a la red***
    - ***Detección de amenazas: Incluir soluciones de detección y prevención de amenazas inalámbricas WIDS/WIPS para identificar y resolver posibles errores o ataques en la red***
    - ***Firewall***
        - ***Incluir capacidades de filtrado de contenido L4-L7***

        - ***Visibilidad y control a través de Deep Packet Inspection (DPI) con el objetivo de clasificar, bloquear, priorizar o limitar ancho de banda de las aplicaciones.***
        - ***Identificación de categoría de páginas Web.***
        - ***Identificación de reputación de página Web.***
    - ***acceso seguro: Implementar mecanismos de seguridad y segmentación como VLANS, Roles o perfiles***
- ***operación:***
    - ***temperatura: Deben soportar una temperatura de operación entre 0 y 50°C***
    - ***Humedad: Deben soportar una humedad relativa en operación entre 5% y 95%***
    - ***Cumplimiento regulatorio: Debe cumplir con:***
        - ***FCC/ISED***
        - ***CE Marked***
        - ***RED Directive 2014/53/EU***
        - ***EMC Directive 2014/30/EU***
        - ***Low Voltage Directive 2014/35/EU***
        - ***UL/IEC/EN 60950***
        - ***IEC/EN 62368-1***
        - ***EN 60601-1-1, EN60601-1-2***
    - ***Certificaciones: Debe tener las siguientes certificaciones:***
        - ***UL2043 plenum rating***
        - ***Wi-Fi Alliance (WFA):***
        - ***Wi-Fi CERTIFIED a, b, g, n, ac, 6, 7***

- ***WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE)***
- ***WMM, WMM-PS, W-Fi Agile Multiband***
- ***Bluetooth SIG***
- ***Ethernet Alliance (PoE, PD device)***

○ ***Garantía: Del tipo lifetime warranty***

d. RENGLÓN 4: WIRELESS LAN CONTROLLER EN NUBE:

Características técnicas: Se deberá cumplir con las características técnicas que se enuncian a continuación.

- ***Gestión:***
  - ***Características generales:***
    - ***Su despliegue debe ser en nube y su licencia debe ser ofrecida como servicio/suscripción.***
    - ***Debe ser capaz de gestionar y correlacionar eventos de la red inalámbrica y cableada (de la misma fábrica)***
    - ***La solución deberá ofrecer la capacidad de escalar mediante arquitectura de microservicios desplegada en proveedores de nube pública como AWS y/o Azure y/o GCP garantizando alta disponibilidad y cumplimiento GDPR.***
    - ***La solución de gestión debe ofrecer acceso a la administración de los dispositivos de red por consola web y no limitar el número de sesiones a la misma***
    - ***Debe contar con una interface fácil de utilizar***
    - ***La solución debe proveer información histórica con disponibilidad de al menos 1 mes de información***
    - ***Deberá detectar posibles problemas que afecten el***

rendimiento de la red y ofrecer pistas sobre la causa raíz del problema para ayudar al administrador en la resolución (Operaciones asistida por IA)

- ***Debe permitir a los usuarios buscar clientes, dispositivos e infraestructura conectada a la red, además deberá proporcionar búsqueda de documentación para ayudar a los usuarios a operar eficienteme sus redes. El motor de búsqueda debe utilizar lenguaje natural para analizar consultas y devolver resultados relevantes.***
- ***Deberá poder definir perfiles de acceso para distintos tipos de usuarios de tal manera que se puedan asignar distintos privilegios de acceso a cada una de las secciones o módulos de la consola.***
- ***En caso de perder conectividad hacia la plataforma de gestión los equipos de la red cableada e inalámbrica deben permitir su operación con la última configuración que recibieron de la nube.***

- ***Montenitoreo:***
  - ***La solución debe contar con una interface fácil de utilizar.***
  - ***La solución debe mostrar información actualizada sobre el uso de la red y métricas de rendimiento de la misma.***
  - ***Debe poder mostrar el mapa topológico de la conexión de un cliente en particular, mostrando la interconexión de los dispositivos de red y los puertos de interconexión. En el caso de los clientes inalámbricos debe ser capaz de indicar la velocidad de conexión y la banda de RF que está siendo utilizada.***
  - ***Debe proveer vistas de red de cada dispositivo (por ejemplo, puntos de acceso, switches, etc) bajo su gestión.***
  - ***En el caso de la red inalámbrica para cada dispositivo o***

radio se deberá contar cómo mínimo con información sobre la cantidad de dispositivos conectados, ancho de banda (bajada y subida), modelo y versión de software, utilización de canales, ruido, pérdidas, errores y retransmisiones, dirección IP, serie, y dirección MAC.

- ***En el caso de la red cableada para cada dispositivo deberá contar cómo mínimo con información sobre modelo, serie, dirección MAC, dirección IP, versión de software, estado de puertos (estado, utilización de subida y bajada, vlans configuradas, información de paquetes unicast, multicas, broadcast, errores y descartes), PoE consumido y disponible, utilización de CPU y memoria, estado de ventiladores y fuentes.***
- ***Debe proveer información sobre los clientes inalámbricos y cableados conectados a los dispositivos de red gestionados como:***
- ***En el caso de los clientes inalámbricos se deberá mostrar como mínimo el nombre de usuario o hostname, dirección IP, MAC, vlan, estado (en línea, fuera de línea o fallido especificando el por qué) radio y canal de conexión inalámbrica, velocidad, throughput de subida y bajada.***
- ***En el caso de los clientes cableados se deberá mostrar como mínimo el nombre de usuario o hostname, dirección IP, MAC, vlan, puerto y switch al cual está conectado, throughput de subida y bajada.***

- ***Visibilidad:***
  - ***La plataforma realizará la identificación y clasificación automática de clientes IoT basado en atributos y motores de IA para análisis de comportamiento. También tendrá la opción para que el administrador defina sus propias clasificaciones con base en criterios como fabricante, sitio, función o categoría.***

- ***La solución deberá ofrecer la capacidad de incorporar monitoreo de equipos de otros fabricantes garantizando visibilidad y control sobre entornos heterogéneos.***
- ***El sistema deberá contar con la capacidad de integrar la información de la salud de red con la experiencia real del usuario***

- ***configuración:***
  - ***El sistema deberá ser capaz de integrarse mediante APIs con plataformas de terceros***
  - ***El sistema deberá permitir de aplicar configuraciones globales, por sitio o por dispositivo, permitiendo cambios escalables y flexibles.***
  - ***Deberá ser posible usar perfiles reutilizables que se propaguen automáticamente a múltiples dispositivos y sitios, asegurando consistencia.***
- ***Diagnóstico y alertas:***
  - ***Debe permitir la habilitación y configuración de alertas***
  - ***Las alertas deben poder ser categorizadas por severidad***
  - ***Las alertas deben poder ser enviadas por correo electrónico***
  - ***Las capacidades de solución de problemas incluyen eventos en vivo, captura de paquetes, registros y herramientas de línea de comando enriquecidas. También están disponibles comprobaciones de diagnóstico, como pruebas de ping y rutas de seguimiento, así como pruebas de rendimiento a nivel de dispositivo.***
  - ***Debe ofrecer extensibilidad con otras plataformas y soluciones de TI a través de API y webhooks, para permitir por ejemplo, automatizaciones de red, interacción con***

herramientas de tiquetes, etc.

- ***Administración de configuraciones y firmware:***
  - ***La plataforma deberá poder hacer cambios de configuración en la infraestructura de red ya sea de manera global, por grupos de equipos o de manera específica a un dispositivo en particular.***
  - ***Debe ser capaz de generar una plantilla de configuración o grupo de configuración. Este debe poder ser aplicada a uno o varios dispositivos de red.***
  - ***Debe proporcionar el aprovisionamiento sin contacto permitiendo un flujo de trabajo simple e intuitivo para configurar los Puntos de Acceso, sin necesidad de participación de TI en el sitio. Los parámetros de configuración se pueden definir según los requisitos específicos de la red o del sitio.***
  - ***Debe proveer información de auditoría para todos los cambios realizados en la red que incluya el nombre del usuario que hizo el cambio así como la fecha/horas y detalle del cambio.***
  - ***Debe proveer la opción de actualizar el firmware de uno o más dispositivos a la vez de manera inmediata o programada.***
  - ***Se debe poder definir versiones de firmware mínimas aceptables por tipo de equipamiento o grupo de dispositivos.***
  - ***Debe indicar si es que hay una versión de firmware superior a la utilizada en los dispositivos. Asimismo, se debe recomendar una versión de firmware por tipo de dispositivo.***
- ***Seguridad:***

- ***La solución debe estar implementada en datacenters que cumplan con las mejores prácticas de seguridad y operación que aseguren el cumplimiento de regulaciones y certificaciones como: SOC, PCI DSS, ISO 27001, GDPR.***
- ***Deberá tener la capacidad de integrar de forma nativa los principios de Zero Trust***
- ***Deberá poder clasificar el grado de confianza de las aplicaciones que se identifiquen en la red y ofrecer geolocalización de las mismas. Se deberá garantizar la capacidad de monitorear más de 3.700 aplicaciones con integración con proveedores de reputación externos, identificando riesgos de seguridad, tendencias de uso y priorización de servicios críticos.***
- ***El sistema deberá permitir condensar miles de flujos de tráfico IoT en un conjunto mínimo de reglas de acceso mediante IA, simplificando la seguridad y reduciendo esfuerzo manual.***

○ ***Reportes:***

- ***La solución deberá generar y programar reportes,***
- ***Los reportes deberán poder generarse y enviarse vía correo electrónico de manera diaria, semanal o mensual.***
- ***Los reportes generados deberán poder ser exportados en formato pdf o csv***
- ***Se deberá garantizar la capacidad de generar informes de conectividad, salud de red y aplicaciones, inventario, uso y planeación de capacidad.***
- ***Los reportes podrán tener un alcance de información global o por sitio***

○ ***Diagnósticos automáticos y recomendaciones:***

- ***La plataforma realizará análisis del desempeño de la red y brindará recomendaciones para su mejora***
- ***El sistema podrá generar recomendaciones contextuales para optimización de roaming, cobertura RF y ahorro energético.***
- ***El sistema deberá contar con la capacidad de generar logs en tiempo real, realizar pruebas de red (ping, traceroute, rendimiento) y enviar esta información directamente al soporte técnico.***

○ ***NAC***

- ***La plataforma integrará funcionalidades de Network access control donde se podrán configurar políticas de acceso con proveedores de identidad en Nube, direcciones MAC o listas de visitantes.***
- ***El sistema deberá permitir autenticar usuarios mediante EAP-TLS, MAC Auth, Captive Portal y MPSK, con integración a IDPs externos como Google Workspace, Entra ID y Okta.***
- ***La solución deberá ser capaz de crear perfiles de autenticación dependiendo de los métodos utilizados. Deberá poderse asignar dichos perfiles a una o varias redes.***
- ***Deberá poder crear políticas de autorización que cumpla una o varias reglas para brindar o denegar acceso y asignarle un distintivo único en la red que identifique la función/tipo del dispositivo final***

○ ***Portal captivo: La solución deberá integrar portal captivo personalizable.***

○ ***Mapas de Calor: El sistema podrá ubicar APs automáticamente sobre el plano con GPS/FTM, generar mapas de calor y con base***

en análisis realizados generar recomendaciones sobre la optimización de la cobertura de red.

e. *RENGLÓN 5: CONTROLADOR DE ACCESO A LA RED (NAC) PARA 1000 USUARIOS CONCURRENTES CON SOPORTE A CINCO (5) AÑOS:*

Características técnicas: Se deberá cumplir con las características técnicas que se enuncian a continuación.

- ***Capacidad: La solución deberá manejar hasta 1.000/10.000/50.000 sesiones RADIUS activas concurrentes por cada appliance (en este caso gestionará 1000)***
- ***Servicios incluidos en licenciamiento base: Deberá incluir en el licenciamiento base los siguientes servicios:***
  - ***802.1X***
  - ***Autenticación por MAC Address***
  - ***TACACS+***
  - ***Enforcement a través de SNMP***
  - ***Perfilamiento de dispositivos***
  - ***Integraciones con terceros mediante REST APIs***
- ***Seguridad contextual: La política de seguridad deberá permitir tomar en consideración elementos contextuales como: horario, ubicación, tipo de dispositivo, versión de SO y nombre del dispositivo, entre otros***
- ***Hardware/Software: Disponible en versión "appliance" de propósito específico.***
- ***Soporte Multivendor: Soporte para Assessment de postura, perfilamiento y autenticación web en ambientes de red multi-vendor y basado en protocolos estándar RADIUS y RADIUS CoA***

- ***Control de acceso unificado: Deberá controlar el acceso de usuarios y dispositivos a través de la red cableada (switches), inalámbrica (access points y controladores WiFi) y VPN (firewalls y concentradores VPN) de manera unificada.***
- ***Servicios AAA: Deberá soportar la aplicación de políticas contextuales mediante servicios AAA: RADIUS, RADIUS CoA, TACACS+ y SNMP***
- ***Reportería: Deberá incluir sin costo adicional un componente de monitoreo y reportería con información en tiempo real e histórica sobre usuarios y dispositivos conectados, alertas, detalle de autenticación y autorización, consumo de anchos de banda***
- ***Métodos de Perfilamiento: Deberá soportar los siguientes métodos de perfilamiento:***
    - ***Activo: Nmap, WMI, SSH, SNMP***
    - ***Pasivo: MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, Puerto 'SPAN', HTTP User-Agent, IF-MAP***
    - ***Integrados y de terceros: Desde la solución de BYOD y de chequeo de postura, EMM/MDM, Rapid7, Cisco device sensor.***
- ***Certificados digitales:***
    - ***La solución deberá ser capaz de actuar como entidad certificadora Root o Intermediaria.***
    - ***Acceso de externos via Portal Cautivo (Invitados, contratistas, clientes)***
- ***Funcionalidades clave:***
    - ***Deberá proveer la opción de autoregistro con confirmación de cuenta vía impresión de ticket, SMS o e-mail, para asegurar que los datos ingresados por los usuarios serán válidos***
    - ***Deberá permitir que antes de que un usuario externo se pueda conectar, el acceso deba ser aprobado por un usuario corporativo (auto-registro con sponsor)***

- ***Deberá permitir que la validez de las cuentas de invitados sea configurable en base a tiempo, anchos de banda utilizados, horario de conexión, entre otros***
- ***Deberá permitir la personalización total del portal cautivo con logos, publicidad, videos, encuestas, etc***
- ***Deberá proveer la opción de acceder a la red a través de las redes sociales Facebook, Twitter, linkedin y Google***
- ***Deberá ajustar de manera automática el tamaño del portal, de acuerdo al dispositivo con el cual se conectan los usuarios.***
- ***Deberá proveer encriptación del tráfico sobre una red abierta mediante el estándar PEAP-Public***
- ***Deberá permitir la asignación de políticas de acceso basadas en roles, para poder asegurar anchos de banda, acceso a recursos específicos y duración de las conexiones, de acuerdo al tipo de invitado***
- ***Deberá permitir la integración con sistemas gestión de huéspedes, pacientes y cobro, tales como: Micros Opera PMS, Protel PMS, Silverbyte Optima PMS, Agilysis Visual One PMS, etc***
- ***Deberá permitir realizar Caching de direcciones MAC por cierta cantidad de tiempo, para evitar que los usuarios recurrentes tengan que introducir constantemente sus credenciales***
- ***Deberá permitir asignar accesos basados en roles a los operadores que crean o modifican las cuentas de usuarios***

- ***Protocolos y Frameworks soportados:***
  - ***Protocolos para los servicios AAA. La solución deberá soportar al menos los siguientes protocolos para los servicios AAA:***
    - ***RADIUS, RADIUS CoA, TACACS+, autenticación web, SAML 2.0***
    - ***EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)***

- ***PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS. EAP-PEAP-Public,EAP-PWD)***
- ***TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5,PAP, CHAP)***
- ***EAP-TLS***
- ***PAP, CHAP, MSCHAPv1 y 2, EAP-MD5***
- ***OAuth2***
- ***Autenticación de Máquina en dominio Windows***
- ***SMB v2/v3***
- ***Autenticación vía MAC (para dispositivos que no soportan 802.1x)***
- ***Online Certificate Status Protocol (OCSP)***
- ***SNMP generic MIB, SNMP private MIB***
- ***Common Event Format (CEF), Log Event Extended Format (LEEF)***

○ ***Fuentes de autenticación: La solución deberá soportar las siguientes fuentes de autenticación sin licenciamiento o plugins adicionales:***

- ***Microsoft Active Directory***
- ***RADIUS***
- ***Cualquier directorio basado en protocolo LDAP***
- ***MySQL, Microsoft SQL, PostGRES, Oracle 11g y cualquier servidor SQL ODBC-compliant***
- ***Servidores de Token***
- ***Base de datos interna***
- ***Kerberos***

- ***Microsoft Azure Active Directory (viaSAML y OAuth2.0)***
- ***Google G Suite***

- ***Estándares RFC: El sistema deberá soportar los siguientes estándares RFC:***
  - ***RFC 2246 The TLS Protocol Version 1.0***
  - ***RFC 2248 Network Services Monitoring MIB***
  - ***RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP***
  - ***RFC 2408 ISAKMP***
  - ***RFC 2409 The Internet Key Exchange (IKE)***
  - ***RFC 2548 Microsoft Vendor-specific RADIUS Attributes***
  - ***RFC 2759 Microsoft PPP CHAP Extensions, Version 2***
  - ***RFC 2865 Remote Authentication Dial In User Service (RADIUS)***
  - ***RFC 2866 RADIUS Accounting***
  - ***RFC 2869 RADIUS Extensions***
  - ***RFC 2882 Network Access Servers Requirements: Extended RADIUS Practices***
  - ***RFC 3079 Microsoft Point to Point Encryption***
  - ***RFC 3576 Dynamic Authorization Extensions to RADIUS***
  - ***RFC 3579 RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)***
  - ***RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines***
  - ***RFC 3748 Extensible Authentication Protocol (EAP)***

- ***RFC 3779 X.509 Extensions for IP Addresses and AS Identifiers***
- ***RFC 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs***
- ***RFC 4137 State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator***
- ***RFC 4301 Security Architecture for IP***
- ***RFC 4302 IP Authentication Header***
- ***RFC 4303 IP Encapsulating Security Payload (ESP)***
- ***RFC 4308 Cryptographic Suites for IPsec***
- ***RFC 4346 TLS Protocol***
- ***RFC 4514 Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names***
- ***RFC 4518 Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation***
- ***RFC 4809 Reqs for IPsec Certificate Mgmt Profile***
- ***RFC 4849 RADIUS Filter Rule Attribute***
- ***RFC 4851 EAP-FAST***
- ***RFC 4945 PKI Profile for IKE/ISAKMP/PKIX***
- ***RFC 5216 The EAP-TLS Authentication Protocol***
- ***RFC 5246 The Transport Layer Security (TLS) Protocol***
- ***RFC 5280 Internet X.509 Public Key Infrastructure***
- ***RFC 5281 EAP-TTLSv0***
- ***RFC 5282 Authenticated Encryption and IKEv2***
- ***RFC 5755 Internet Attribute Certificate Profile for***

Authorization

- *RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*
- *RFC 6818 Updates to the Internet X.509 Public Key*
- *RFC 6960 X.509 Internet Public Key Infrastructure*
- *RFC 7030 Enrollment over Secure Transport*
- *RFC 7296 Internet Key Exchange Protocol Version 2*
- *RFC 7321 ESP y AH*
- *RFC 7468 Textual Encodings of PKIX, PKCS, and CMS Structures*
- *RFC 7815 Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation*
- *RFC 8032 Edwards-Curve Digital Signature Algorithm (EdDSA)*
- *RFC 8247 The Internet Key Exchange v2 (IKEv2)*

○ *Servicios adicionales: Deberá tener la capacidad de adicionar de manera modular servicios de: Portal Cautivo, enrolamiento de dispositivos personales en entornos corporativos (BYOD) y Postura de Seguridad sobre PCs corporativos*

○ *Licenciamiento: El licenciamiento deberá ser perpetuo.*

○ *Integración con soluciones de terceros: Deberá tener la capacidad de integración vía REST-based APIs, de manera nativa y sin costo adicional de licenciamiento, con soluciones de Seguridad Perimetral (Ej: CheckPoint, Palo Anto, Fortinet, etc), MDM/EMM (Ej: Citrix, MobileIron, AirWatch), sistemas de gestión de tickets (Ej: Service Now, y múltiples factores de autenticación (Ej: DUO, RSA SecurID), UEBA (IntroSpect)*

○ *Segmentación dinámica: Se requiere que la solución aplique el*

control de acceso y segmentación dinámica basada en roles, para evitar el uso de múltiples VLANs para aplicar políticas de seguridad

- ***Perfilamiento de dispositivos: La solución deberá soportar perfilamiento para despliegues con direccionamiento IP fijo***
- ***Social Login: La solución deberá soportar autenticación via social login con Facebook, Linkedin, Google y Twitter X***
- ***Integraciones del portal cautivo: El portal cautivo deberá ser capaz de integrarse con soluciones de PMS, pago por uso y publicidad***
- ***Privilegios sobre los dispositivos: Se requiere que la solución pueda aplicar políticas de acceso, perfilamiento y autenticación sin necesidad de habilitar privilegios de administración sobre los equipos***
- ***Perfilamiento de dispositivos: Se requiere que la solución pueda perfilar y categorizar los dispositivos que se conectan a la red sin licenciamiento adicional***
- ***Single Sign On: La solución deberá soportar SAML tanto como SP e IdP y el protocolo Oauth para habilitar Single Sign On con aplicaciones y portales externos***
- ***Fuentes de Autenticación: La solución deberá soportar bases de dato SQL como fuente de autenticación sin necesidad de agregar licenciamiento o plugins adicionales***
- ***Portal cautivo: El portal cautivo deberá ser altamente personalizable***
- ***Certificados digitales: La solución deberá ser capaz de actuar como entidad certificadora Root o Intermediaria.***

6. CALIDADES

Todos los bienes que conforman la solución cuya contratación se propicia estarán constituidos por unidades nuevas, sin uso previo, originales de fábrica y en perfecto estado de conservación. La adjudicataria será plenamente responsable por cualquier defecto de fabricación, incumplimiento de normativa, o vicio oculto que se detecte, debiendo proceder a su reemplazo inmediato sin costo adicional para la jurisdicción.

La jurisdicción se reserva el derecho de rechazar el equipamiento que no cumpla con las especificaciones técnicas, sin que ello genere derecho a reclamo alguno por parte de la adjudicataria.

7. GARANTÍA:

La solución deberá contar con la garantía que se indique para cada renglón que comprende la presente contratación.

8. FECHA Y LUGAR DE ENTREGA:

La entrega se acordará con las jurisdicción con una anticipación mínima de CUARENTA Y OCHO (48) horas y, en principio, se realizará de 10 a 17 horas, en las oficinas del MINISTERIO DE JUSTICIA sitas en Sarmiento N° 329 y Cochabamba N° 54 de la CIUDAD AUTÓNOMA DE BUENOS AIRES.

9. FORMA DE COTIZACIÓN:

Los interesados deberán realizar sus propuestas teniendo en miras la totalidad de los requisitos técnicos detallados en las presentes Especificaciones Técnicas.

10. FORMA DE ADJUDICACIÓN:

Por razones logísticas y para garantizar la correcta provisión y respaldo de los bienes, la adjudicación se realizará de manera global a un único oferente.

Fernando La Iglesia
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412

Ricardo Orsi
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412