Superintendencia de Notariado y Registro

ANEXO No. 2 - ESPECIFICACIONES TÉCNICAS - LOTE DOS

SUPERINTENDENCIA DE NOTARIADO Y REGISTRO
OFICINA DE TECNOLOGIAS DE LA INFORMACION - OTI

OBJETO:

ADQUISICIÓN Y RENOVACIÓN DE EQUIPOS DE CONECTIVIDAD WIRELESS, CONTROL DE ACCESO, INCLUYENDO LICENCIAMIENTO, SOPORTE Y GARANTÍA.

JULIO, 2025

Superintendencia de Notariado y Registro

Tabla de contenido

INTRODUCCIÓN 3
1. IDENTIFICACIÓN DEL CLASIFICADOR DE BIENES Y SERVICIOS 4
2. ALCANCE DEL OBJETO LOTE 2 4
3. CONTEXTO Y CARACTERISTICAS DE LA PLATAFORMA DE CONECTIVIDAD WIRELLESS ARUBA 4
3.1. ADQUISICIÓN Y RENOVACIÓN DE EQUIPOS ARUBA, INCLUYENDO SOPORTE Y GARANTÍA PARA LOS DISPOSITIVOS DE CONECTIVIDAD WIRELESS ARUBA ACTUALES 4
4. ESPECIFICACIONES TÉCNICAS MÍNIMAS PARA RENOVACIÓN DE EQUIPOS ARUBA: 8
5. ESPECIFICACIONES TÉCNICAS MÍNIMAS PARA ADQUISICIÓN DE EQUIPOS ARUBA: 11

Superintendencia de Notariado y Registro

INTRODUCCIÓN

La Superintendencia de Notariado y Registro (SNR) juega un papel crucial en el fortalecimiento de la confianza ciudadana hacia el Estado, actuando como garante de la tradición de los derechos de la propiedad y la validez de ciertos actos civiles. Esta confianza se basa en la certeza de que las actuaciones del Registro de Instrumentos Públicos se alinean con el orden jurídico y reflejan fielmente la voluntad de las partes involucradas. Para lograr esto, es imperativo que la superintendencia y las oficinas de registro empleen herramientas eficientes y seguras que faciliten el acceso a los servicios registrales.

En este contexto, el Decreto 2723 de 2014 encarga a la SNR la asesoría al Gobierno Nacional en la formulación de políticas públicas y el desarrollo de programas y planes en el ámbito de los servicios públicos registral y notarial. Además, la ley 1579 de 2012, en su artículo 6, subraya la importancia de unificar los sistemas de registro de la propiedad inmueble a nivel nacional mediante el uso de tecnologías digitales y procedimientos técnicos avanzados, para asegurar un proceso de registro seguro, rápido y eficaz.

La SNR ha emprendido un proceso de modernización de sus procesos misionales, apoyándose en tecnologías de la información y comunicaciones (TIC), esto incluye infraestructura de Seguridad que permite proteger tanto los sistemas de información, como los datos que se crean, transmiten, procesas o almacenan en los mismos.

Este esfuerzo de modernización se alinea con las directrices del Manual de implementación de la Política de Gobierno Digital y la ley 2294 de 2023 (PND), que buscan mejorar la relación Ciudadano-Estado y hacer interoperable la información a través del Sistema de Administración de Tierras (SAT), el repositorio de datos maestros (RDM) y la consolidación del Catastro Multipropósito.

Finalmente, la entidad se ha propuesto como objetivo estratégico convertirse en un modelo de excelencia en la prestación de servicios públicos registral y notarial, liderando los procesos de protección, restitución y formalización de la recuperación de tierras. Este objetivo se apoya en una plataforma tecnológica moderna y un talento humano fortalecido, para satisfacer la demanda cambiante de los servicios asociados y garantizar el acceso oportuno a la información de propiedad inmobiliaria en todo el territorio nacional, independientemente de la ubicación geográfica de las Oficinas de Registro.

1. IDENTIFICACIÓN DEL CLASIFICADOR DE BIENES Y SERVICIOS

El presente proceso está codificado en el clasificador de bienes y servicios UNSPSC como se indica en la siguiente Tabla.

Código	Segmento	Familia	Clase
43222600	Difusión de tecnologías de información y Comunicaciones.	Equipos o plataformas y accesorios de redes multimedia o de voz o de datos.	Equipos de servicio de red.
43223300	Difusión de tecnologías de información y comunicaciones.	Equipos o plataformas y accesorios de redes multimedia o de voz o de datos.	Dispositivos y equipos para instalación de conectividad de redes y datacom.
43222500	Difusión de tecnologías de información y Comunicaciones.	Equipos o plataformas y accesorios de redes multimedia o de voz o De datos.	Equipo de seguridad de red.
81161700	Servicios basados en ingeniería, investigación y Tecnología	Entrega de servicios de tecnología de información.	Servicios de telecomunicaciones.

2. ALCANCE DEL OBJETO

ADQUISICIÓN Y RENOVACIÓN DE EQUIPOS DE CONECTIVIDAD WIRELESS, CONTROL DE ACCESO, INCLUYENDO LICENCIAMIENTO, SOPORTE Y GARANTÍA – Lote 2.

3. CONTEXTO Y CARACTERISTICAS DE LA PLATAFORMA DE CONECTIVIDAD WIRELLESS ARUBA

3.1. ADQUISICIÓN Y RENOVACIÓN DE EQUIPOS ARUBA, INCLUYENDO SOPORTE Y GARANTÍA PARA LOS DISPOSITIVOS DE CONECTIVIDAD WIRELESS ARUBA ACTUALES.

Es necesario ampliar la infraestructura de conectividad inalámbrica (WLAN) en la sede central de la SNR con el fin de optimizar la cobertura y mejorar la calidad del acceso a la red, aprovechando que la entidad ya cuenta con la solución Aruba, se fortalecerá el esquema de puntos de acceso de la red Wi-Fi, asegurando una mayor eficiencia en la

conectividad. Esta ampliación garantiza la compatibilidad tecnológica y permite una administración unificada, simplificando la gestión y el soporte de la red.

La renovación del licenciamiento, soporte y garantía de la plataforma Aruba en la SNR es una decisión estratégica fundamental para asegurar la continuidad, seguridad y eficiencia en la conectividad de los usuarios. Además de garantizar la protección frente a vulnerabilidades, esta medida permite robustecer la infraestructura Wi-Fi existente, mejorando la capacidad de la red y su rendimiento.

La plataforma Aruba ofrece funcionalidades críticas para el correcto funcionamiento y control de acceso a las redes y sistemas de información de la entidad, tales como la gestión avanzada de accesos, monitoreo en tiempo real y detección proactiva de amenazas. Así mismo, con esta actualización, se optimiza el esquema de red, permitiendo una administración centralizada y eficiente que asegura la disponibilidad y estabilidad de los servicios, alineándose con las necesidades crecientes de conectividad y seguridad de la SNR.

PLATAFORMA DE SEGURIDAD – CONTROL ACCESO A LA RED ARUBA:

La plataforma NAC (Network Access Controller) o Control de Acceso a la Red, proporciona seguridad y control de acceso para dispositivos en redes empresariales. Permite gestionar y asegurar el acceso a la red para usuarios y dispositivos, ya sean con cable, inalámbricos o VPN.

Con el licenciamiento renovado se establece una capa base de protección para la infraestructura tecnológica de la entidad, teniendo en cuenta que brindan varios servicios de seguridad clave como:

1. **Autenticación y Autorización:**
   - La plataforma autentica usuarios y dispositivos utilizando múltiples métodos de autenticación, como 802.1X, RADIUS, LDAP, Active Directory y bases de datos internas.
   - Proporciona control de acceso basado en roles, asegurando que solo los usuarios y dispositivos autorizados puedan acceder a los recursos de la red.

2. **Gestión de Políticas:**
   - Los administradores pueden definir políticas granulares basadas en una amplia variedad de atributos, como tipo de dispositivo, ubicación, hora del día, y tipo de conexión.
   - Las políticas pueden aplicarse de manera dinámica, adaptándose a las condiciones cambiantes de la red y del entorno de seguridad.

3. **Onboarding de Dispositivos:**

- ClearPass facilita el proceso de incorporación segura de nuevos dispositivos a la red (BYOD - Bring Your Own Device).
- Proporciona portales de auto-registro y aplicaciones de configuración para que los usuarios puedan conectar sus dispositivos de manera segura.

4. **Visibilidad y Análisis:**
   - Ofrece visibilidad detallada de todos los dispositivos conectados a la red, incluyendo información sobre el tipo de dispositivo, sistema operativo, y estado de cumplimiento.
   - Proporciona herramientas de análisis y reportes que ayudan a los administradores a monitorear el comportamiento de la red y detectar posibles amenazas.

5. **Integraciones:**
   - La solución NAC se integra con una amplia gama de soluciones de seguridad y gestión de TI, como firewalls, sistemas de gestión de dispositivos móviles (MDM), y plataformas de gestión de eventos de seguridad (SIEM).
   - Estas integraciones permiten una respuesta coordinada a incidentes de seguridad y una gestión unificada de políticas.

De acuerdo con las características de las plataformas descritas anteriormente, se considera fundamental realizar la renovación del soporte, licenciamiento y garantía para asegurar lo siguiente respecto a sus servicios:

- Renovar el licenciamiento y la garantía que es crucial para mantener la funcionalidad y seguridad de los dispositivos.
- Renovar el soporte proporcionará soluciones y apoyo de primer nivel para la entidad en caso de incidentes, dudas o apoyo en la gestión de las soluciones.
- Garantiza el acceso a actualizaciones de software, parches de seguridad y nuevas características que pueden mejorar el rendimiento y la protección contra amenazas.
- La garantía proporciona protección contra fallas del hardware y la posibilidad de obtener reemplazos o reparaciones sin costo adicional, lo que ayuda a garantizar la continuidad del negocio.

ACCESS POINTS ARUBA:

Con base a los diagnósticos ejecutados en el edificio de la sede central de la Superintendencia, se identificaron áreas con baja cobertura y con exceso de conexiones, por lo que se requiere un incremento en la capacidad **con 8 nuevos Access Point (AP) Aruba**, con los cuales se aumentará la cobertura de la red inalámbrica, permitiendo una distribución más eficiente del tráfico de red. Esto es fundamental para áreas con alta

densidad de dispositivos conectados simultáneamente, donde los AP actuales pueden verse saturados.

Balanceo de carga y mejor rendimiento: Al aumentar la cantidad de access points, se logrará un balanceo de carga más efectivo. La red podrá distribuir equitativamente las conexiones entre los nuevos y los existentes, reduciendo la congestión en puntos críticos y mejorando el rendimiento general de la red.

Redundancia y alta disponibilidad: La adición de nuevos AP introduce redundancia en la red, lo que es vital para mantener la conectividad en caso de fallos o mantenimiento en alguno de los dispositivos actuales. Esto incrementa la alta disponibilidad de la red, asegurando que los servicios críticos de la SNR no se vean interrumpidos por problemas de infraestructura.

Compatibilidad con Wi-Fi 6: Los nuevos AP Aruba son compatibles con los últimos estándares de conectividad inalámbrica, incluyendo Wi-Fi 6 (802.11ax), lo que mejora la velocidad, eficiencia y capacidad de la red. Esto es especialmente importante para soportar la creciente demanda de ancho de banda generada por aplicaciones de alta intensidad como videoconferencias, transmisión de datos en tiempo real y sistemas de gestión documental.

Seguridad avanzada: Los AP Aruba ofrecen características avanzadas de seguridad, como segmentación de red dinámica, detección de intrusiones (IDS), y protección contra ataques man-in-the-middle. Estos elementos son esenciales para proteger los datos sensibles de la SNR, garantizando que la infraestructura inalámbrica esté alineada con los estándares de ciberseguridad actuales.

Gestión centralizada y monitoreo en tiempo real: Con la ampliación del número de AP, la plataforma de gestión Aruba Central permitirá la monitorización en tiempo real de todos los puntos de acceso, así como la configuración remota de los mismos. Esto facilita la detección y resolución de problemas de conectividad antes de que afecten a los usuarios, optimizando la operación diaria de la red.

Escalabilidad futura: La adquisición de 8 AP no solo satisface las necesidades actuales, sino que también prepara la red para futuros incrementos en la cantidad de usuarios y dispositivos conectados, sin necesidad de reemplazar la infraestructura actual. Esto representa una solución escalable y preparada para el crecimiento de la SNR en los próximos años.

Reducción de interferencias y mejor calidad de señal: Al contar con más AP distribuidos estratégicamente, se mejora la calidad de la señal y se minimizan las interferencias entre dispositivos, especialmente en entornos con alta densidad de conexiones. Esto optimiza la

experiencia de los usuarios finales al mantener conexiones más estables y de mayor velocidad.

Soporte para dispositivos IoT: Los nuevos AP están preparados para soportar un mayor número de dispositivos IoT (Internet de las Cosas), los cuales están en constante aumento dentro de las instituciones. La capacidad de manejar estos dispositivos sin afectar el rendimiento de la red principal es clave para la transformación digital de la SNR.

Reducción del tiempo de latencia y mejora en la calidad del servicio (QoS): La mayor densidad de access points reduce la latencia, lo que es fundamental para aplicaciones sensibles al tiempo, como videollamadas y transmisión de datos en tiempo real. Además, el sistema de Quality of Service (QoS) de Aruba prioriza el tráfico más importante, asegurando que los servicios críticos de la SNR mantengan su calidad y disponibilidad.

En conclusión, la adquisición de los 8 nuevos access points Aruba no solo complementa la infraestructura actual, sino que también fortalece la red de la SNR, preparándola para enfrentar los desafíos tecnológicos presentes y futuros. Esta inversión es clave para asegurar una conectividad óptima, mantener la seguridad de los datos y mejorar la experiencia de los usuarios, al tiempo que se optimizan los recursos tecnológicos de la entidad.

Por lo tanto, la plataforma Aruba es clave para garantizar una conectividad y seguridad óptimas para los dispositivos que se conectan a las redes de la Superintendencia y renovar su licenciamiento y garantía es una inversión estratégica y fundamental para mantener su funcionalidad y proteger la inversión en tecnología ejecutada por la Entidad.

4. ESPECIFICACIONES TÉCNICAS MÍNIMAS PARA RENOVACIÓN DE EQUIPOS ARUBA:

Comentado [JV1]: VALIDAR SI ES LA MISMA INFO

Ítem	Cantidad	Descripción
1	2	Renovación Soporte técnico para las máquinas virtuales (VM) de la solución Clearpass por un año (Seriales XHBP6V89452C y XHX9M2BC6475)
2	1	Renovación de soporte técnico y garantía para 1000 licencias Access de clearpass (Seriales XHN6C397F8B2) por un año
3	2	Renovación Soporte técnico y garantía de las controladoras Appliance Wireless Aruba 7205 por un año (CS0024269 - CS0024285)
4	20	Renovación Soporte técnico y garantía de los Access Point Aruba AP-555 por un año
TOTAL	25	

De acuerdo con lo anterior las especificaciones técnicas mínimas y su respectiva descripción para la renovación de equipos, licencias y servicios de soporte para las soluciones Aruba son las siguientes:

Producto	Requerimiento		Unidad de medida
Soporte Técnico y Garantía - Clearpass	Soporte técnico de fábrica de máquinas virtuales (VM) de la solución Clearpass por un año.		Soporte y garantía para 2 máquinas virtuales de la solución clearpass
Soporte y Garantía – Licencias Access	Renovación de soporte técnico y garantía para 1000 licencias Access de clearpass.		**Soporte y garantía para 1000 licencias**
Soporte y Garantía – Controladora Wireless Aruba	Renovación soporte técnico y garantía de las controladoras Wireless Aruba 7205 por un año		**Soporte y garantía para 2 controladoras Aruba 7205**
Soporte y garantía – Access Point Aruba	Renovación soporte técnico y garantía para los Access point Aruba AP-555 por un año con los siguientes seriales:	• VNN3K9Y0PP • VNN3K9Y0NL • VNN3K9Y0NV • VNN3K9Y0MX • VNN3K9Y0MH • VNN3K9Y0NT • VNN3K9Y0KY • VNN3K9Y0KS • VNN3K9Y0LJ • VNN3K9Y0Q2 • VNPXK9Y0CL • VNPXK9Y0CM • VNPXK9Y0D6 • VNPXK9Y0DS • VNPXK9Y0DV • VNPXK9Y0GK • VNPXK9Y0GT • VNPXK9Y0GW • VNPXK9Y0H7 • VNPXK9Y0H8	**Soporte y garantía para 20 AP Aruba-555**
Servicios de Soporte y servicios profesionales.	• La solución NAC deberá ser desplegada por parte del proponente con reglas de control de acceso y configuraciones suficientes para proteger la infraestructura tecnológica de la Superintendencia. • Servicio de soporte por parte del proveedor o canal con modalidad 7x24x365 con tiempo de respuesta de solicitudes (primer contacto) no superior a 1 hora. • El servicio de soporte sobre las plataformas debe incluir acompañamiento y consultas sobre funcionamiento o configuraciones de los servicios y requerimientos de soporte por cualquier medio (correo electrónico, sesiones remotas y atención en sitio en caso de requerirse). • Soporte ante cualquier falla presentada sobre las soluciones Aruba indicadas en este anexo técnico.		Servicios de Soporte y servicios profesionales.

Producto	Requerimiento	Unidad de medida
	• Apoyo en la actualización y migración a las últimas versiones liberadas por el fabricante de las soluciones de Aruba indicadas en este anexo técnico. • Apoyo en nuevas configuraciones, parametrizaciones sobre las soluciones Aruba indicadas en este anexo técnico. • Afinamientos sobre las soluciones de Aruba indicadas en este anexo técnico. • Creación de nuevos reportes y/o configuración de reglas y alertas para detectar incidentes y/o vulnerabilidades. • Asistencia en la resolución de problemas y análisis de la causa raíz de estos cuando sea necesario sobre las soluciones Aruba. • Apoyo en el escalamiento de casos de soporte con el fabricante Aruba. Cualquier otro requerimiento que se solicite sobre el portafolio de soluciones de Aruba.	
Transferencia de Conocimiento	**SOLUCIÓN NAC:** • Transferencia de conocimiento de mínimo 20 horas, respecto a la administración de las soluciones Aruba indicadas en este anexo técnico en su última versión disponible, que permitan administrar las herramientas con suficiencia, una vez las plataformas sean actualizadas. • La transferencia de conocimiento deberá ser para 3 personas. **SOLUCIONES DE CONECTIVIDAD WIRELESS:** • Transferencia de conocimiento de mínimo 20 horas, respecto a la administración de las soluciones Aruba indicadas en este anexo técnico en su última versión disponible, que permitan administrar las herramientas con suficiencia, una vez las plataformas sean actualizadas. • La transferencia de conocimiento deberá ser para 3 personas.	20 horas de transferencia de conocimiento – Solución NAC

Producto	Requerimiento	Unidad de medida

Entregables	• Matriz de Escalamiento de Soporte.
	• Documento con la situación actual de las soluciones (assessment) y mejoras a realizar en la plataforma.
	• Plan de Trabajo que incluya las siguientes actividades:
	  ○ Cronograma de actividades para actualización de las soluciones Aruba indicadas en este anexo técnico.
	  ○ Cronograma para ejecución de mejoras y puesta a punto a realizar en las soluciones Aruba indicadas en este anexo técnico.
	• Registro de asistencia y certificado individual para cada asistente a las transferencias de conocimiento que se dicten
	• Memorias de la transferencia de conocimiento.
	• Grabaciones de la transferencia de conocimiento realizada para la SNR.
		Documentación

5. ESPECIFICACIONES TÉCNICAS MÍNIMAS PARA ADQUISICIÓN DE EQUIPOS ARUBA:

A continuación, se relacionan las especificaciones técnicas mínimas y su respectiva descripción para la adquisición del fortalecimiento del esquema tecnológico de los dispositivos Aruba para la SNR:

Comentado [JV2]: Colocar los dispositivos AP a adquirir por modelo y/o especificación técnica

Ítem	Cantidad	Descripción
1	8	Adquisición Access Points AP-510 Aruba para interiores orquestados por la controladora Aruba con la que cuenta la entidad.
TOTAL	8	

De acuerdo con lo anterior las especificaciones técnicas mínimas y su respectiva descripción para la adquisición de equipos, licencias y servicios de soporte para las soluciones Aruba son las siguientes:

Comentado [OC3R2]: Ok. Sugerencia incluida

REQUISITOS TÉCNICOS SOLUCIÓN EQUIPOS WIFI
ESPECIFICACIONES TÉCNICAS
Se renovará el esquema de red de Access Points Aruba para interiores orquestados por la controladora Aruba con la que cuenta la entidad. Las características mínimas de los Access Points, deben cumplir con las siguientes condiciones: No se aceptarán soluciones OEM, los APs, Controladora y Software deberán ser nativos fabricados por la marca. **1.2.1 TECNOLOGÍA INALÁMBRICA** • 4x4 MIMO

- Soporte para doble banda 802.11ax con OFDMA y MU-MIMO.
- Data rates mínimo de 4 Gbps en 5Ghz y 575Mbps en 2.4Ghz.
- Tecnología four spatial stream.
- Soporte Wi-Fi Multimedia (WMM).
- Soporte Bluetooth 5 y radios Zigbee para casos de usos de IOT y servicios delocalización.
- Al menos 16 SSID por radio.
- Soporte de asociación de mínimo 256 clientes por radio.
- Asignación y selección de canal de manera automática, así como los niveles de potenciadel AP
- Con el fin de evitar problemas asociados a sticky clients, la plataforma debe contar con mecanismos automáticos que migren a los clientes hacia el punto de acceso con el mejor nivel de servicio en todo momento, basado en información de ubicación del cliente, capacidades del dispositivo cliente, condiciones del entorno RF y congestión de los puntos de acceso, sin que requiera intervención del usuario y que aplique a las distintas marcas y modelos de dispositivos presentes en el mercado.

1.2.2 ESTÁNDARES IEEE Y CERTIFICACIONES

Los APs deben soportar al menos los siguientes estándares de la industria:

- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n
- IEEE 802.11ac BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
- 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
- 802.11ac very high throughput (VHT) support: VHT20/40/80/160
- IEEE 802.3af/at/bt clase 3 o superior
- IEEE 802.3 az

1.2.3 INTERFACES

- Un interfaz RJ-45 10/100/1000BASE-T autosensing con capacidad de soportaralimentación eléctrica vía estándar PoE 802.3at/bt clase 3 o 4.
- Interface USB 2.0 (Conector Tipo A)
- Radio Bluethoot 5 y Zigbee (802.15.4)
- Botón de reset
- Interface consola serial

1.2.4 CONECTIVIDAD WIRELESS

Tasas de Transmisión al menos (Mbps):

- 802.11b: 1, 2, 5.5, 11
- 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
- 802.11n: 6.5 to 300 (MCS0 to MCS15, HT20 to HT40)
- 802.11ac: 6.5 to 3467 (MCS0 to MCS9, NSS = 1 to 4, VHT20 to VHT160)
- 802.11ax (2.4GHz): 3.6 to 574 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE40)
- 802.11ax (5GHz): 3.6 to 4803 (MCS0 to MCS11, NSS = 1 to 8, HE20 to HE160)

1.2.5 MODOS DEL AP

El AP deben estar en capacidad de operar al menos en los siguientes modos:

- Como equipo AP stand-alone.
- Como equipo AP controlado al integrarse a un Wireless Access Controller.
- Los APs ofertados deberán tener la capacidad de ser administrados desde la Nube sin necesidad de agregar algún hardware adicional.
- Los APs deberán tener la capacidad de operar en modo controlado usando su propio sistema operativo, sin necesidad de una controladora física, ni licencias adicionales.
- Debe contar con mecanismos que permitan Zero Touch Provisioning para implementación automática al contar con una conexión a Internet sin intervención de serviciotécnico especializado.

1.2.6 ANTENAS

- Al menos cuatro antenas omnidireccionales dual band descendente MIMO con ganancia de 4.2dbi en 2.4GHz y 7.5dbi en 5Ghz
- Bandas de frecuencia seleccionables por software para cada radio.
- Reducción de interferencia co-canal

1.2.7 SEGURIDAD

El AP debe incluir al menos soporte para:

- Algoritmo de cifrado: WPA, WPA2 y WPA3.
- Servicios de seguridad para identificación, clasificación y bloqueo de IPs, archivos o URLs maliciosos.
- Capacidad de manejar roles por usuario y políticas basadas en identidad.
- WMM o WMM-PS.
- Chip para aseguramiento de plataforma confiable TPM
- Cliente VPN.
- Integración con solución de NAC. El fabricante deberá contar con solución de control deacceso Enterprise de la misma marca, para poder implementar a futuro esta solución. No se requiere ofertar licenciamiento para NAC.

1.2.8 ALIMENTACIÓN ELÉCTRICA Y SOPORTES

Cada Access Point debe incluir su respectivo inyector PoE basado en el estándar 802.3at ysoporte para el montaje físico.

1.2.9 CERTIFICACIONES Y REGULACIONES

Los APs deben cumplir al menos con las siguientes:

- UL2043 plenum rating
- Wi-Fi Alliance:
  - Wi-Fi CERTIFIED a, b, g, n, ac, ax
  - WPA, WPA2 and WPA3
  - Enterprise with CNSA option
  - Personal(SAE), Enhnced Open (OWE)
  - WMM, WMM-PS, W-Fi Agile Multiband

- Passpoint (release 2) • Bluetooth SIG • FCC/ISED • CE Marked • RED Directive 2014/53/EU • EMC Directive 2014/30/EU • Low Voltage Directive 2014/35/EU • UL/IEC/EN 60950 • EN 60601-1-1, EN60601-1-2
INSTALACIÓN
• Se deben instalar según mapa de calor con el que cuenta la SNR. • La Entidad entregara la conexión a cero metros para la instalación de los APs. • El oferente debe realizar la configuración de los APs y la asociación a la controladora existente propiedad de la Entidad. • El proponente debe adjuntar carta del fabricante que lo acredite como canal.
GARANTIA
• Contrato de servicios por un (1) año garantizando el correcto funcionamiento de los equipos activos, actualizaciones ilimitadas de software durante la vigencia de la garantía y soporte 7x24 remoto, telefónico y/o presencial si es requerido. • Derecho a actualizaciones ilimitadas (UPDATE y UPGRADE) de las versiones de software entregadas durante un (1) año, provisto directamente por el fabricante a la entidad. • Tiempo de Respuesta Telefónica inmediato.

Nota: El contratista debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que su personal asignado al proyecto pueda cumplir con las obligaciones del contrato. Estos valores no incurrirán en costos adicionales para la Superintendencia de Notariado y Registro.

Cordialmente,

JOSE RICARDO ACEVEDO SOLARTE
Jefe de la Oficina de Tecnologías de la Información

Elaboro y proyecto: Juan Carlos Valenzuela Buitrago – Contratista OTI
Martha Milena Rueda – Grupo Servicios Tecnológicos
Reviso: Oscar Fabian Corredor Camargo – Coordinador Grupo Servicios Tecnológicos