DESCRIPCIÓN GENERAL

Nomenclatura	Significado
ID. General	Estándar Equipo Tecnológico CI-13-2024
CI-E52	Estándar de puntos de acceso (AP) de alta gama para interiores
20240202	Fecha de actualización

Modelos de referencia

En febrero del 2024 se verificó este estándar frente a los siguientes equipos del mercado.

- ✓ Meraki CW9166-MR

DESCRIPCIÓN TÉCNICA

A partir de este punto es la descripción técnica a utilizar en el proceso de compra correspondiente, copie a partir de este punto.

----------**Inicio de descripción técnica**----------

Referencia: CI- E52-20240202 (favor no remover o modificar esta referencia)

1. **Características básicas del equipo**
   - 1.1. El equipo debe operar tanto en la banda de 2.4GHz como en la banda de 5GHz y 6GHz.
   - 1.2. El equipo debe permitir modificar la potencia de transmisión tanto para 2.4 GHz, 5 GHz y 6GHz.
   - 1.3. El dispositivo deberá ser compatible y estar configurado para ser controlado desde la nube. El dispositivo también debe tener la flexibilidad de ser manejado en premisas mediante una controladora en caso de ser requerido.
   - 1.4. El equipo debe contener antenas integradas con las siguientes características:
     - 1.4.1 Para 2.4 GHz, una antena interna omnidireccional en azimut con una ganancia de 3 dBi.
     - 1.4.2 Para 5 GHz, una antena interna omnidireccional en azimut con una ganancia de 5 dBi.
     - 1.4.3 Para 6 GHz, una antena interna omnidireccional en azimut con una ganancia de 4 dBi.
   - 1.5. Debe contar con las siguientes Interfaces:
     - 1.5.1 Una interfaz de 10/100/2.5/5G BASE-T Ethernet (RJ-45).
     - 1.5.2 Un conector de alimentación de DC (8 mm centro positivo).
     - 1.5.3 USB 2.0 at 4.5W
   - 1.6. Debe contar con los siguientes indicadores: LED de estado indicando el estado del encendido, estado de arranque y estado de actualización del firmware.

1.7. El dispositivo debe incluir una tecnología que permita reducir los puntos muertos de manera automática y mejorar la disponibilidad de las conexiones de los clientes.

1.8. El equipo debe contar con una tecnología que permita detectar la interferencia y ofrecer capacidades de análisis de espectro.

1.9. El equipo debe incorporar una tecnología que permita mejorar el rendimiento de la conexión hacia los dispositivos móviles, para asegurar una utilización mínima de la batería en teléfonos Wireless VoIP.

1.10. El equipo debe incorporar una tecnología que permita a los clientes con capacidad triple banda de preferir la banda de 6GHz o 5Ghz en lugar de la banda de 2.4 GHz.

1.11. El equipo debe incorporar optimización de RF automático basado en nube, permitiendo sintonizar automáticamente la selección de canales, la potencia de transmisión y la configuración de la conexión del cliente.

1.12. El equipo debe contar con tecnología Bluetooth para visibilidad y escaneo de dispositivos cercanos.

2. Características técnicas

2.1. El equipo debe soportar las capacidades de 802.11ax, 802.11ac Wave 2 y 802.11n:

2.1.1 DL-OFDMA, UL-OFDMA, compatibilidad con TWT, coloración BSS

2.1.2 Entrada múltiple 4 x 4, salida múltiple (MIMO) con cuatro flujos espaciales

2.1.3 Combinación de relación máxima (MRC) y formación de haces

2.1.4 Compatibilidad con SU-MIMO, UL MU-MIMO y DL MU-MIMO

2.1.5 Canales de 20 y 40 MHz (802.11n)

2.1.6 Canales de 20, 40 y 80 MHz (802.11ac Wave 2)

2.1.7 Canales de 20, 40, 80 y 160MHz (802.11ax)

2.1.8 Hasta 1024-QAM en bandas de 2,4 GHz, 5 GHz y 6 GHz

2.2. Debe cumplir con los estándares IEEE:

2.2.1 802.3 ab/bz

2.2.2 802.3 af/at/bt

2.2.3 802.11a/b/g/n/

2.3. El equipo debe manejar características de multimedia tipo Wi-Fi

Multimedia (WMM™).

2.4. El punto de acceso debe contar con las siguientes certificaciones:

2.4.1 WiFi 6 (R2), WiFi 6E, WPA3-R3, WPA3-Suite B, Enhanced Open Security

2.4.2 Bluetooth Low Energy

2.5. El dispositivo debe incluir tecnología 4x4:4 múltiple entrada – múltiple salida (MIMO) basada en el estándar 802.11ax, con cuatro corrientes espaciales, con capacidad de radio triple de hasta 7.78 Gbps.

2.6. El equipo debe soportar los siguientes radios:

2.6.1 Radio de acceso de cliente 802.11b/g/n/ax de 2,4 GHz.

2.6.2 Radio de acceso de cliente 802.11a/n/ac/ax de 5 GHz.

2.6.3 Radio de acceso de cliente 802.11ax de 6 GHz.

2.6.4 WIDS/WIPS de triple banda de 2,4 GHz, 5 GHz y 6 GHz, análisis de espectro y radio de análisis de ubicación.

2.6.5 Radio Bluetooth Low Energy (BLE) de 2,4 GHz con baliza y soporte de escaneo.

2.6.6 Funcionamiento simultáneo de las cuatro radios.

2.7. Bandas de frecuencia admitidas (se aplican restricciones específicas de cada país):

2.7.1 2.484 GHz

2.7.2 5.250 GHz (UNII-1)

2.7.3 5.350GHZ (UNII-2A)

2.7.4 5.490 - 5.730 GHz (UNII-2C)

2.7.5 5,735 -5,825 GHz (UNII-3)

2.7.6 5.925–6.425 GHz (UNII-5)

2.7.7 6.425–6.525 (UNII-6)

2.7.8 6.525–6.875 (UNII-7)

2.7.9 6.875–7.125 (UNII-8)

2.8. El equipo debe soportar las siguientes características de alimentación:

2.8.1 Alimentación a través de Ethernet: 42,5 - 57 V (compatible con 802.3at)

2.8.2 Alternativa: entrada de 54 V DC

2.8.3 Consumo de energía: 30.5 W max (con soporte USB) o 25 W max (sin soporte de USB)

3. **Aspectos de seguridad**

3.1. Debe cumplir con los siguientes estándares de seguridad:

3.1.1 802.11i, WPA2-PSK, WPA2-Enterprise, WPA3 – Personal, WPA3 – Enterprise, WPA3 - Enhanced Open (OWE).

3.1.2 802.1X

3.1.3 Advanced Encryption Standards (AES).

3.2. El equipo debe soportar los siguientes Tipos de EAP:

3.2.1 EAP-Transport Layer Security (TLS)

3.2.2 EAP-Tunneled TLS (TTLS)

3.2.3 Protected EAP GTC (PEAP)

3.2.4 EAP-Subscriber Identity Module (SIM)

3.3. El equipo debe soportar las siguientes funcionalidades de seguridad:

3.3.1 Cortafuegos de capa 7 integrado con gestión de políticas de dispositivos móviles

3.3.2 WIDS/WIPS en tiempo real con alertas y contención automática de puntos de acceso no autorizados con Air Marshal

3.3.3 Acceso flexible para invitados con aislamiento de dispositivos

3.3.4 Etiquetado de VLAN (802.1q) y tunelización con IPsec VPN

3.3.5 Informes de cumplimiento de PCI

3.3.6 Integración de gestión de movilidad empresarial (EMM) y gestión de dispositivos móviles Características de seguridad

3.4. Debe cumplir con los siguientes estándares de seguridad:

3.4.1 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA

3.4.2 802.1X

3.4.3 Advanced Encryption Standards (AES).

3.4.4 El equipo debe soportar las siguientes funcionalidades de seguridad:

3.4.5 Cortafuegos de capa 7 integrado con gestión de políticas de dispositivos móviles

3.4.6 WIDS/WIPS en tiempo real con alertas y contención automática de puntos de acceso no autorizados con Air Marshal

3.4.7 Acceso flexible para invitados con aislamiento de dispositivos

3.4.8 Etiquetado de VLAN (802.1q) y tunelización con IPsec VPN

3.4.9 Informes de cumplimiento de PCI

3.4.10 Integración de gestión de movilidad empresarial (EMM) y gestión de dispositivos móviles (MDM)

3.5. El equipo debe soportar los siguientes Tipos de EAP:

3.5.1 EAP-Transport Layer Security (TLS)

3.5.2 EAP-Tunneled TLS (TTLS)

3.5.3 Protocol Versión 2 (MSCHAPv2)

3.5.4 Protected EAP (PEAP) v0 o EAP-MSCHAPv2

3.5.5 EAP-Subscriber Identity Module (SIM)

4. Normas y estándares de soporte

4.1. CSA y CB 60950 y 62368

4.2. Cumple con UL 2043

4.3. EN 61001

4.4. El dispositivo debe contar con las siguientes aprobaciones de Radio:

4.5. Canadá: FCC parte 15C, 15E RSS-247

4.6. EN 300 328 (v2.1.1)

4.7. EN 301 893 (v2.1.1)

4.8. Australia/Nueva Zelanda: AS/NZS 4268

4.9. México: NOM-208

4.10. Taiwán: NCC LP0002

4.11. El equipo debe incluir el licenciamiento para ser gestionado por el sistema de administración y monitoreo operativo, se debe cumplir con las siguientes características:

4.12. Gestión de la nube.

4.13. Actualizaciones de firmware sin intervención.

4.14. Aprovisionamiento sin contacto.

4.15. Soporte de API.

4.16. Integración de Bluetooth y ESL con SES-imagotag (compatible con puntos de acceso con la radio IoT).

4.17. Funciones de seguridad como Air Marshal, reglas de firewall de capa 3 y capa 7.

4.18. Se debe incluir el licenciamiento por un periodo de 5 años.

5. Características del sistema de Administración y Monitoreo Operativo:

5.1. Gestión y control centralizados en la forma de una consola de administración basada en Web desde la cual se deberá poder acceder, configurar y monitorear todos los puntos de acceso Inalámbricos WiFi considerados en este estándar.

5.2. La gestión y control debe ser un sistema basado en nube, como servicio del fabricante de los equipos propuestos, y el equipo también deberá tener la capacidad de ser administrado en premisas.

5.3. La gestión deberá ser un sistema que contenga redundancia de hardware y geográfica en su implementación, y deberá ser capaz de administrar al menos 25,000 equipos físicos.

5.4. El acceso a la consola central deberá ser por HTTPS y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet

5.5. Capacidad de registrar y desplegar los equipos de forma automática, basado en su número serial u otro identificador, para otorgarles su configuración y versión de sistema operativo correspondientes

5.6. La conectividad con los equipos gestionados deberá ser de una forma segura (encriptada).

5.7. Durante la vida del contrato, los equipos propuestos deberán poder recibir sus parches y actualizaciones de software, empujados de forma centralizada y calendarizarles conforme sea requerido.

5.8. Los equipos propuestos deben tener la capacidad de mantenerse operativo en caso de perder conectividad con el portal de administración en la nube.

5.9. Deberán existir mecanismos para agrupar lógicamente la administración de un número determinado de dispositivos inalámbricos WiFi, para propósitos de realizar cambios simultáneos en sus configuraciones y tener homogeneidad de estas.

5.10. De igual manera, desde la consola de administración basada en Web, se deberán poder generar los reportes de utilización históricos, así como datos de su uso en tiempo real, correspondientes a todos los dispositivos inalámbricos WiFi, ya sea individual o grupal.

5.11. La consola deberá ser accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones usando navegadores de Internet populares y en versiones aún soportadas por el mismo desarrollador

5.12. El acceso a la consola de administración deberá ser capaz de realizarse mediante un método de autenticación de dos factores (two-factor authentication), incluyendo, mas no limitado, a nombre de usuario y contraseña más una app de soft-token en dispositivos móviles.

5.13. La consola deberá de tener controles que fuercen a los administradores a: cambiar contraseña periódicamente, limitar la reutilización de contraseñas pasadas, implementar contraseñas robustas, congelar sus cuentas en casos repetidos de ingreso incorrecto de contraseña y sacarlos de la consola en caso de inactividad.

5.14. Deberá haber una bitácora de quién y a qué hora han intentado entrar al sistema de gestión, incluyendo dirección IP de proveniencia y locación estimada.

5.15. Deberá haber una bitácora de quién, hora y qué cambios se hicieron a las configuraciones de los equipos gestionados por medio de tal plataforma.

5.16. La consola de gestión debe tener la capacidad de limitar las peticiones de ingreso provenientes de direcciones IP especificadas.

5.17. Deberá de haber un mecanismo para medir el ancho de banda entre los equipos y el sistema de gestión centralizado.

5.18. Soporte de SAML para poder ingresar a la plataforma de gestión mediate uso de credenciales institucionales.

5.19. La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles y permisos diferenciados.

5.20. Deberá soportar la interacción programática mediate interfases de programación de aplicativos RESTful (RESTful APIs) que sean abiertas, utilizando HTTPS para transporte y JSON para serialización de objetos, con repositorios públicos demostrables de código reutilizable.

5.21. La consola central tendrá capacidad de ser fuente de información SNMPv3 consolidada de los dispositivos que gestiona.

5.22. La consola deberá mostrar un inventario de los dispositivos que gestiona, mostrando al menos el número serial, dirección MAC y si está desplegado o no.

5.23. La consola deberá mostrar el estado detallado de licenciamiento de cada dispositivo que gestiona.

5.24. Deberá mostrar una lista de los distintos sitios que tengan equipos, cantidad de éstos en línea y fuera de línea, así como un conteo de dispositivos usuarios y volumen de datos consumidos

5.25. La herramienta de monitoreo será capaz de visualizar por sitio un perfilamiento de los dispositivos que hayan usado la red, mostrando al menos su nombre, sistema operativo, fabricante, direcciones MAC e IP y uso en volumen de datos, todo en hasta al menos 30 días

5.26. La herramienta de monitoreo será capaz de visualizar las aplicaciones utilizadas por los dispositivos del punto anterior, proveyendo una lista con volumen de datos y cantidad de dispositivos que hayan hecho uso de tales aplicaciones en hasta al menos 30 días

5.27. De los puntos anteriores, la herramienta deberá mostrar una gráfica de utilización de ancho de banda en hasta al menos 30 días que pueda ayudar para propósitos de planeación de capacidad

5.28. La herramienta de gestión central permitirá entrar al detalle individual de cada dispositivo que ha usado la red para conocer a detalle su historial de navegación

5.29. Se podrán hacer capturas de paquetes directamente desde la herramienta de gestión, en cualquiera de los dispositivos gestionados y en cualquiera de sus interfases

5.30. La solución de gestión / monitoreo deberá mostrar toda actividad de navegación que cruza la infraestructura gestionada, incluyendo aplicaciones usadas, con dominios visitados o direcciones IP’s de sitios, el protocolo usado, el volumen de datos en total dividido en enviado y recibido, la cantidad de flujos, tiempos activos, y su cantidad de usuarios, todo en hasta 30 días de uso.

5.31. Adicionalmente:

5.31.1 El equipo debe debe incluir el licenciamiento para ser gestionado por el sistema de administración y monitoreo operativo, se debe cumplir con las siguientes características

5.31.2 Gestión de la nube

5.31.3 Actualizaciones de firmware sin intervención

5.31.4 Aprovisionamiento sin contacto

5.31.5 Soporte empresarial 24x7 y RMA

5.31.6 Soporte de API

5.31.7 Integración de Bluetooth y ESL con SES-imagotag (compatible con puntos de acceso con la radio IoT)

5.31.8 Meraki Salud

5.31.9 Integración NBAR (se aplican requisitos mínimos de firmware y hardware)

5.32. Funciones de seguridad como Air Marshal, reglas de firewall de capa 3 y capa 7

5.33. Se debe incluir el licenciamiento por un periodo de 5 años.

6. Otras características:

6.1. Un cable (patch cord) mínimo categoría 6A de 1 metro

6.2. Un cable (patch cord) mínimo categoría 6A de 3 metros

6.3. Un candado similar a Candado Essential YALE/ 20mm con las siguientes características:

6.3.1 Candado de bronce macizo 20mm

6.3.2 Gancho de acero endurecido

6.3.3 Sistema de cierre de doble anclaje

6.3.4 Combinación de 3 pines de bronce

6.3.5 Grado de Seguridad: Medio

6.3.6 Nivel de Corrosión: para humedad

6.3.7 Incluye 3 llaves

6.3.8 Terminación: Bronce liso

6.4. Los equipos deben ser 100% compatibles con la nube de gestión de telecomunicaciones Meraki que está vigente en la Universidad de Costa Rica.

----------**Fin de descripción técnica**----------

APARTADO DE ACCESORIOS Y EQUIPAMIENTO OPCIONAL A CONSIDERAR

Se excluye de la definición formal del estándar las características relacionadas con componentes y/o accesorios adicionales tales como:

a) n/a

Dado que los requerimientos de cada usuario varían de acuerdo a necesidades específicas, la unidad solicitante de la compra deberá determinar las características de los componentes y/o accesorios adicionales que se requieren. En caso de ser necesario, el Centro de Informática puede brindar la asesoría correspondiente.

RESPONSABLE Y REVISIONES:

Actividad	Rol
Elaboración	Xiomara Céspedes Jiménez, Colaboradora Unidad de Gestión de Adquisiciones (UGA) Rebeca Esquivel Flores , Coordinadora Área de Gestión de Comunicaciones (AGC)
Revisión y visto bueno	Cindy Arias Quiel, Coordinadora (UGA)
Aprobación	**Tatiana Bermúdez Páez, Subjefa CI**

UCR Firmado digitalmente