UNIVERSIDAD AUTONOMA
DE MADRID

Pliego de prescripciones técnicas para el arrendamiento, con opción a compra, de una nueva red inalámbrica para la Universidad Autónoma de Madrid

1 Objeto del Pliego

El presente pliego tiene por objeto describir los trabajos a realizar y las características de los equipos a arrendar por la Universidad Autónoma de Madrid, para conseguir una infraestructura de red inalámbrica renovada, de tecnología moderna, con buena cobertura para todos los dispositivos que a ella se conectan, y que proporcione un buen servicio a todos los usuarios de la universidad. Asimismo, se detallan las condiciones del mantenimiento de la nueva infraestructura.

2 Antecedentes.

2.1 Instalación inicial.

La actual red inalámbrica de la Universidad Autónoma de Madrid (UAM), se instaló entre finales de 2005 y principios de 2006.

El equipamiento adquirido fue de la marca Alcatel-Lucent, pero, realmente, eran productos fabricados por Aruba Networks, puesto que entonces Aruba no vendía sus productos directamente en España.

Se instalaron casi quinientos AP70, con sus correspondientes rosetas de cableado, proporcionando cobertura únicamente en el interior de los edificios, con una fuerza de señal mínima de -80dB en la banda de 2,4GHz, y una relación señal/ruido de 20dB.

Se instalaron y configuraron dos instancias de FreeRADIUS y la red se adhirió a la iniciativa internacional Eduroam[1].

2.2 Ampliaciones.

Desde 2006 en adelante se han ido añadiendo APs de varios tipos, AP70, AP105 y AP225, para mejorar la cobertura o el rendimiento de los usuarios en algunos espacios: salas de lectura, salones de actos, cafeterías, aulas de portátiles, etc.

También se ha ido añadiendo algún edificio nuevo. El edificio C de la EPS fue dotado de AP70 en 2009, y la Plaza Mayor fue dotada de AP105 en 2012. Entre 2012 y 2014 se instalaron cuatro AP175 de exterior, sin utilizar conexiones *mesh*.

2.3 Actualización.

En el año 2013 se actualizaron las controladoras. Se adquirieron dos OAW-4650, equipos equivalentes a los 7220 de Aruba.

Hasta 2015 las controladoras proporcionaban el servicio DHCP y direccionamiento IP público a los clientes inalámbricos. Desde 2015, el servicio DHCP lo proporciona el equipamiento Infoblox de la universidad, y los *firewalls* de Palo Alto dan el servicio de NAT. También, desde ese año, los clientes se reparten automáticamente entre las ocho *VLANes* en las que está dividida, a nivel 2, la red inalámbrica.

[1] www.eduroam.org y www.eduroam.es

2.4 Proyecto piloto.

Para ver los posibles problemas y las consideraciones técnicas que deberían tenerse en cuenta a la hora de hacer una actualización completa de la red inalámbrica de la UAM, en 2015 se llevó a cabo un proyecto piloto de actualización, que consistió en la actualización de la red inalámbrica con los parámetros que ahora se estiman más recomendables en dos zonas del campus:

- La Facultad de Derecho.
- Dos módulos de la Facultad de Ciencias.

En ambas localizaciones, durante el piloto, se han instalado APs del modelo AP205 con los nuevos parámetros de cobertura y se retiraron los AP70.

También se adquirió una tercera controladora OAW-4650.

El fin principal de los nuevos parámetros de cobertura es proporcionar una buena señal a los teléfonos móviles y a las tabletas, y dejar la red preparada si se quisiera utilizar para VoIP sobre red inalámbrica. Se presentan a continuación los valores más significativos de los nuevos objetivos de cobertura.

- 5GHz como banda de estudio.
- Fuerza de señal mínima -63dBm.
- Relación señal/ruido mínima 25dB.

En el Colegio Mayor Juan Luis Vives, que originalmente disponía de unos pocos AP70 en cafetería, biblioteca y salón de actos, se instalaron treinta AP205 para dar cobertura a las habitaciones. No se instalaron realizando estudios de cobertura. Los AP70 existentes se mantuvieron.

La conclusión principal de este proyecto piloto es que el ratio de sustitución de cada AP instalado en 2005/2006 es 3 a 1. Este dato es orientativo, sin que en ningún caso constituya una regla exacta. El número de APs a instalar en cada zona vendrá marcado por el estudio previo de cobertura.

2.5 Conmutadores de red cableada.

Los conmutadores de la red cableada de la UAM, que dan servicio a la red inalámbrica, también son muy antiguos. En su gran mayoría están fuera de mantenimiento por el fabricante, y son muy pocos los que proporcionan bocas de 1Gbs de velocidad y alimentación PoE+ (802.3at).

3 Situación actual.

Se describe a continuación la situación del equipamiento central de la red y la distribución actual de APs en los edificios de la universidad.

3.1 Controladoras.

- Dos OAW-4650 con versión de *software* 6.3.x para soportar los AP70, que aún siguen siendo el equipo mayoritario en la red. Los AP70 no son soportados por las versiones 6.4 o superiores. Comparten un pack de 500 licencias AP+PEF+WIP.

- Un OAW-4650 con versión de *software* 6.4.x para soportar los nuevos AP205 instalados en 2015, y los AP105. Los AP205 no son soportados por versiones 6.3 o inferiores. Dispone de un pack de 500 licencias AP+PEF+WIP.

Las tres controladoras disponen de fuente de alimentación redundante y un SFP+ 10Gb SR cada una.

3.2 Equipos AAA.

La universidad dispone actualmente de dos instancias de FreeRADIUS, como *software* AAA (*Authentication, Authorization* y *Accounting*), que son usadas por la red inalámbrica, algunos equipos de la red cableada y el servicio de VPN.

Están instaladas en la plataforma de virtualización VMware de la universidad y están adheridas al árbol de RADIUS de la iniciativa europea Eduroam.

En el Anexo I se describe el sistema de virtualización de la universidad.

3.3 Gestión.

La universidad dispone de un Omnivista 3600, que es el equivalente al Airwave de Aruba. Está instalado en la plataforma de virtualización VMware de la universidad antes descrita y dispone de 900 licencias.

El Omnivista se utiliza para obtener informes, registrar la calidad del servicio, ver los tráficos que se demandan y los dispositivos que se usan en la red inalámbrica. No se utiliza para gestionar las controladoras.

Por un problema de capacidad y rendimiento, el Omnivista solo almacena los datos de sesiones de usuarios del último mes. Y por ese mismo motivo, sólo guarda los contadores necesarios para elaborar informes de los últimos dos o tres meses.

De esta forma, los servicios técnicos de la universidad, con el Omnivista/Airwave pueden:

- Ver la calidad de servicio y el detalle de cada una de las conexiones de usuarios del último mes.
- Ver los tráficos y máquinas conectadas de la red inalámbrica.
- Mantener mapas de la distribución de APs por el campus.
- Elaborar informes de tipos y modelos de máquinas que se conectan, APs con más usuarios, APs con más tráfico, usuarios más pesados, distribución de dominios de los usuarios que se conectan, aplicaciones más utilizadas por los clientes Wi-Fi, etc.

El Omnivista actual ya tiene incorporados los planos de la gran mayoría de los edificios con la situación de los APs. Gracias a eso, es capaz de mostrar los valores de cobertura con "mapas de calor".

3.4 Accounting.

La universidad dispone de una máquina que almacena los registros de inicio y fin de las sesiones de los usuarios, durante dos años por lo menos, y con la que se realizan consultas sobre esos registros. La máquina es un Windows Server 2008 sobre la plataforma de virtualización, ya mencionada, de la universidad.

Los FreeRADIUS reciben los inicios y fin de sesión de las controladoras, los reformatean a MySQL, y lo envían las máquinas de almacenamiento.

3.5 Portal de invitados.

La universidad dispone actualmente de un *appliance* de ClearPass Guest:

- ClearPass Policy Manager 500 HW Appliance - RADIUS/TACACS+ server with advanced policy control for up to 500 unique endpoints. (Código Alcatel CP-HW-500)
- Guest License for ClearPass Policy Manager - 100 endpoints (Código Alcatel LIC-CP-GM-100)

3.6 *Software* para estudios de cobertura y resolución de problemas.

Los servicios técnicos de la universidad disponen de un Premium Pack del *software* Ekahau, que fue adquirida en 2014 y contiene lo siguiente:

- Una licencia de Ekahau Site Survey Professional.
- Un Hub USB más 3 antenas NIC300 USB.
- Una licencia DBx Spectrum Analyzer.
- Una antena Wy-Spy USB.
- Una licencia de Mobile Survey para Android 2.1+.

3.7 Equipo de testeo.

La universidad dispone de un Air Check Wi-Fi Tester de Fluke 1.0 a/b/g/n desde 2011. No dispone de ningún tipo de accesorio adicional: antena direccional, batería adicional, etc.

3.8 Distribución actual de APs.

En el Anexo II se expone una lista de la instalación actual por edificios. Se detalla el número actual y modelos de APs instalados en cada armario de comunicaciones, y el tipo de panel de cableado de cada armario.

3.9 Conmutadores.

Los conmutadores actualmente instalados en los armarios de comunicaciones de la universidad, para dar acceso a los usuarios, y para dar PoE y conectividad a los APs actuales, son de la marca Cisco. Los modelos son los que se listan a continuación.

- 3750 y 3750 PoE Fast Ethernet.
- 3750G.
- 3750X y 3750X PoE.
- 2960X.
- 3850-XS.

Están conectados a los conmutadores de distribución y de *core* por medio de interfaces SFP o SFP+.

4 Características de la nueva infraestructura y trabajos a realizar.

El adjudicatario debe suministrar, instalar, configurar y mantener todo el equipamiento necesario, controladoras, APs, *software* de gestión, *software* AAA, *accounting*, portal de invitados, conmutadores de acceso, cableado, etc..., para que la nueva red funcione de la misma forma que la actual en todos sus parámetros, VLANES, QoS, ACLs, etc..

Todo el equipamiento suministrado deberá ser nuevo, y adquirido a través de los canales oficiales del fabricante en España.

4.1 Parámetros de cobertura.

Las mejoras respecto a la instalación del año 2005 y 2006, que se quieren conseguir son las siguientes:

- Una cobertura suficiente para dispositivos móviles y tabletas.
- Utilizar como banda de estudio la de 5GHz.
- Tecnología 802.11ac Wave 2 en los APs.
- Red preparada para VoIP sobre red inalámbrica.

En todas las zonas del interior de los edificios, a excepción de las zonas de parking e instalaciones (transformadores, calderas, etc.), los valores objetivo serán:

- Banda: 5GHz.
- Round Trip Time menor de 100ms.
- Packet loss menor del 1%.
- Velocidad mínima 24Mbps.
- Cobertura RF mayor o igual que -63dBm.
- SNR mayor o igual que 25dB.
- Número de APs: mínimo 2 a un mínimo de -63dBm.

En las zonas de parking e instalaciones los valores objetivo serán:

- Banda: 5GHz.
- *Round Trip Time* menor de 500ms.
- *Packet loss* menor del 10%.
- Velocidad mínima 2Mbps.
- Cobertura RF mayor o igual que -75dBm.
- SNR mayor o igual que 10dB.
- Solapamiento de canales: 3 a -80dBm.

4.2 Estudios de cobertura iniciales y finales.

Con los parámetros del apartado anterior, la empresa instaladora realizará un estudio de cobertura inicial en todos los edificios, para determinar cuál es la mejor localización de los nuevos APs. Los estudios se presentarán a los servicios técnicos de la universidad, antes de la instalación de los nuevos APs, para acordar conjuntamente la disposición más adecuada en cada edificio.

Los nuevos APs se instalarán siempre en las ubicaciones que indiquen los estudios de cobertura. Las ubicaciones de los APs antiguos nunca condicionarán la instalación de los nuevos.

La empresa adjudicataria instalará los nuevos APs, y retirará los antiguos, en coordinación con los servicios técnicos de la universidad, y siempre de forma que la interrupción del servicio sea mínima.

Una vez terminada la instalación y activación de los nuevos APs, y tras retirar los antiguos, la empresa adjudicataria llevará a cabo un estudio de cobertura final en todos los edificios, para verificar que los parámetros de cobertura real corresponden con las especificaciones anteriormente detalladas.

En caso de que en algunas ubicaciones esto no fuese así, la empresa adjudicataria se hará cargo, sin coste para la universidad, de las instalaciones adicionales de puntos de cableado y APs para conseguir los parámetros de cobertura especificados.

Tanto el estudio de cobertura inicial, como el final, se realizarán con la herramienta de análisis de espectro activada, y sus resultados serán presentados a los servicios técnicos de la universidad para su visado y aprobación.

Los estudios de cobertura se llevarán a cabo con el *software* Ekahau. Los ficheros de trabajo de los estudios se entregarán a la universidad.

4.3 Controladoras.

La universidad considera que la topología inalámbrica más adecuada para su campus es el de APs gestionados por controladoras.

Las controladoras que se suministren han de ser obligatoriamente *appliances* físicos. No se admitirá la utilización de controladoras sobre máquinas virtuales.

Se suministrarán tantas controladoras como sean necesarias y, como mínimo, una adicional por redundancia N+1. Serán configuradas por el adjudicatario con la supervisión de los servicios técnicos de la universidad.

En todos los casos, se dotará de las suficientes licencias para soportar todos los APs de la red. Tanto las licencias, como las controladoras, deben permitir funcionalidades de *firewalling* y gestión del espacio radioeléctrico.

4.3.1 Características Mínimas

Las características recogidas en el presente capítulo son de obligado cumplimiento para la tecnología propuesta por el ofertante. El no cumplimiento de alguna de ellas, será motivo de exclusión de la propuesta presentada.

Todas las funcionalidades deben ser realizadas por la controladora sin ayuda de componentes externos.

GENERAL

- Arquitectura WLAN Centralizada con Puntos de Acceso subordinados a la controladora.

- Las controladoras tienen que ser auto-contenidas, integradas sin necesitar de requisitos específicos sobre la electrónica de red.
- La solución planteada debe proporcionar alta disponibilidad, sin punto único de fallo *hardware*.
- "*Sub-second Fail-over*" de punto de acceso.
- "*Sub-second fail-over*" de cliente Wi-Fi.
- Sincronización entre controladoras sin necesidad de ninguna plataforma o servidor externo.
- Solución Wi-Fi basada en estándares 802.11.
- Soporte de conectividad cliente-red, y de extensión de red inalámbrica sin cables (soluciones *Mesh*).
- Hasta 64 SSID simultáneos.
- Soporte de hasta 20.000 dispositivos simultáneos.
- *Roaming* de nivel 3 disponible entre todos los puntos de acceso de la red.
- Priorización de tráfico multimedia WMM o superior.
- Soporte de tráfico *multicast* hacia clientes Wi-Fi.
- Soporte de IPv6 en clientes Wi-Fi.
- Detección automática de la topología de puntos de acceso desplegada, tanto gestionados como extraños (*rogue AP*) o autorizados.
- Asignación automática de canales y potencias de los puntos de acceso gestionados en ambas bandas en función de la topología detectada.
- Monitorización periódica del espectro radioeléctrico con posibilidad de reacción automática al ruido detectado, cambiando de canal los puntos de acceso afectados y los de sus alrededores.
- Tolerancia a fallos. En el caso de que caiga una controladora, los puntos de acceso podrán asociarse a otra que esté activa automáticamente.
- Detección de zonas sin cobertura cuando cae un punto de acceso y posibilidad de aplicación de contramedidas aumentando la señal de los de alrededor.
- Detección y contramedidas ante ataques de seguridad.
- Soporte de localización y rastreo de dispositivos RFID.
- Soporte de sistema de localización y tracking de clientes Wi-Fi.
- Posibilidad de filtrado de clientes por MAC.
- Es de la máxima importancia que la controladora permita el bloqueo completo del tráfico entre las estaciones inalámbricas. Esta funcionalidad debe activarse obligatoriamente.
- Capacidad para sustituir la fuente de alimentación en caliente.

<u>AUTENTICACIÓN Y CIFRADO</u>

- Mecanismos de autenticación.
  - MAC.
  - 802.1X.
  - Web-Based integrado.
- Cifrado.
  - Cifrado WPA2/AES en la capa de enlace.
  - Cifrado WEP en la capa de enlace.
  - Cifrado WPA/TKIP en la capa de enlace.
  - Autenticación LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-GTC.
- Autenticación EAP 802.1X a través de servidores RADIUS y LDAP.
- Posibilidad de usar RADIUS para asignar usuarios o dispositivos a determinados Roles o *VLANs*.

- Autenticación de usuarios centralizada en el controlador que permita un *roaming* rápido del cliente entre dos puntos de acceso incluso si están gestionados por controladoras distintas.
- *Accounting* en servidores RADIUS y en otros sistemas.
- Soporte de autenticación vía usuario y *password*.
- Soporte de autenticación basada en *token*.
- Capacidad de generación de *passwords* temporales y credenciales de invitado que expiren automáticamente.
- Soporte de APIs para control automatizado desde sistemas externos.
- Posibilidad de usar base de datos de usuarios invitados para la autenticación 802.1X.
- Soporte de Walled Garden.

SOPORTE AL ESTÁNDAR 802.11

- Debe soportarse *Wi-Fi Alliance* 802.11a/b/g/n/ac
- Explícitamente debe soportarse, además, 802.11ac *Wave 2*.
- IEEE 802.11d.
- IEEE 802.11h.
- IEEE 802.11i.
- IEEE 802.11k.
- IEEE 802.11r.
- IEEE 802.11w.

COMUNICACIÓN AP-CONTROLADOR.

- Encriptación/desencriptación centralizada, es decir, terminada en la controladora para prevenir captura de tráfico en puntos intermedios.
- Soporte de encriptación/desencriptación en los Puntos de acceso sin la necesidad de hardware específico.
- Soporte de encriptación/desencriptación de extremo a extremo, es decir, la controladora, deberá poder finalizar el túnel de cifrado de los clientes (sin ningún hardware adicional) en lugar de finalizarlo en los puntos de acceso.

GESTIÓN RF

- Capacidad para repartir, inteligente y dinámicamente dispositivos sin recibir una nueva petición de asociación desde el cliente.
- Capacidad de ajustes de Radiofrecuencia manuales y automáticos.
- Capacidad de *beamforming*.
- Soporte de radios certificadas DFS que puedan habilitar 14 canales adicionales en 5GHz.
- Capacidad de modificar o deshabilitar tasas de protocolos 802.11 (por ejemplo 802.11b *data rates*) por SSID, o por otros parámetros.
- Reparto de carga entre bandas y forzado de clientes duales (2.4GHz y 5GHz) hacia la banda de 5GHz, para mejorar el rendimiento global de la red, sin la necesidad de usar ninguna configuración en el cliente, ni pieza de *software (band steering)*.
- Capacidades de *Traffic shaping* para ofrecer *air-time fairness* entre distintos tipos de clientes con diferentes sistemas operativos, en entornos de alta densidad, sin configuración específica en los clientes finales.
- Capacidad de proporcionar acceso preferente a clientes rápidos frente a clientes lentos.
- Gestión de la interferencia co-canal.

- Soporte de Gestión de Radiofrecuencia en tiempo real sin la necesidad de ejecutar ninguna plantilla ni administración manual de medidas, basado en información de tiempo real obtenida de la instalación.
- Redundancia RF.
- Soporte de canales de 40 MHz y agregación de canales.
- Soporte de *20 MHz Short Guard Interval.*
- Posibilidad de gestionar la capacidad/rendimiento por usuario.

CONTROL DE ACCESO

- Forzado (*enforcement*) de la seguridad para usuarios Wi-Fi, mediante el uso de un *firewall*, integrado en la propia controladora, y basado en roles, que puede ser directamente integrado con los roles definidos dentro de los servidores de autenticación.
- De forma dinámica, inspección de los derechos de acceso de los clientes a la red, una vez autenticado, basado en origen, destino y/o puertos.
- Capacidad para asegurar protección de privacidad mediante la prevención de ataques al *firewall* y de IP *spoofing* y forzado de la negociación TCP.
- Las políticas de acceso deben poder proporcionar capturas automáticas de datos y el registro (*syslog*) de las reglas de acceso activadas para auditoria y análisis.
- Reglas para derechos de acceso basadas en cualquier combinación de tiempo, lugar, usuario, dispositivos, y atributos extendidos obtenidos de la base de datos de autenticación.
- El *firewall* de la controladora debe ser capaz de ejecutar políticas automáticas basadas en criterios que den lugar a diferentes acciones: permitir, denegar, rechazar, o enrutar tráfico, hacer NAT por origen o destino del tráfico, modificar el nivel calidad de servicio (*QoS*), y pasar el cliente a una *blacklist* para excluirlo de la red.
- El sistema centralizado de conmutador/controladora debe soportar actualizaciones de roles dinámicos de usuarios basados en mensajes recibidos de *APIs* externas.
- Detección y Filtrado de aplicaciones. Se evita que el cliente Wi-Fi pueda hacer uso de algunas aplicaciones, mediante el filtrado de las comunicaciones que genera.
- Capacidad para registrar los dispositivos que acceden por portal cautivo y/o SSID 802.1X.
- Capacidad para configurar la opción de *pass through* para portal cautivo con varios parámetros: destino, puertos y protocolos IP.
- Debe proporcionar soporte *Bring Your Own Device* (BYOD) y permitir una forma simple, fiable y eficiente de incorporar nuevos clientes a la red.
- Time-based SSID. Posibilidad de aplicar un perfil horario, a la radiación o no de un SSID. Debe poderse establecer con criterio periódico o específico, distinguiendo si se desea entre días laborables y fines de semana.
- Asignación de franjas horarias de disponibilidad del SSID de invitados para mayor seguridad y control.
- Control de la tasa de transferencia de paquetes, basada en el valor establecido del ancho de banda, a invitados individuales, para un mayor control del tráfico de invitados.

Todas y cada una de las controladoras que se suministren deben estar equipadas con:

- Dos fuentes de alimentación.
- Dos interfaces 10GBase-SR.

Es obligatoria la integración de las controladoras con los *firewalls* de Palo Alto de la universidad. Esta integración supone, como mínimo, que las controladoras envíen los identificadores de usuario a los *firewalls* para que éstos puedan establecer políticas de forma más racional.

4.4 Puntos de Acceso (APs)

4.4.1 APs de interior.

4.4.1.1 Características Mínimas comunes

Las características recogidas en el presente capítulo son de obligado cumplimiento para la tecnología propuesta por el ofertante. El no cumplimiento de alguna de ellas, será motivo de exclusión de la propuesta presentada.

Las funcionalidades mínimas que se requieren sobre los APs son las detalladas en el listado de este apartado.

- Todos los APs deberán soportar el estándar 802.11ac Wave 2 con soporte de "*beamforming*" basado en estándares. Así como mantener la compatibilidad con estándares anteriores 802.11 a/b/g/n.
- Los equipos han de ser Dual Band (2'4GHz y 5GHz)
- Las radios deberán poder hacer Análisis de Espectro para detectar interferencias no Wi-Fi y servir clientes de manera simultánea.
- El AP deberá poder detectar y clasificar las fuentes de interferencia externas (Microondas, *bluetooth*, DECT, etc...).
- Todos los APs ofertados deben incorporar radios de última generación con posibilidad de analizar el espectro con una resolución de 5Mhz, para detectar posibles interferencias.
- Soporte para protocolos de eficiencia energética, 802.3az, *Energy Efficient Ethernet.*
- Certificado Wi-Fi Alliance (WFA) 802.11a/b/g/n/ac.
- Soporte de los siguientes métodos de cifrado:
    - CCMP/AES.
    - TKIP.
- Los puntos de acceso deberán incluir filtros para protegerse de las interferencias provocadas por redes 3G/4G.
- *Deep packet inspection* en el mismo AP.
- IEEE 802.11d.
- IEEE 802.11h.
- IEEE 802.11i.
- IEEE 802.11k.
- IEEE 802.11r.
- IEEE 802.11w.
- Soporte de canales UNII-1 (36-48), UNII-2 (52-64), UNII-2 extended (100-140) y UNII-3 (149-161) en el radio de 5GHz.
- Soporte de hasta 16 SSID.
- Botón de *reset*.
- Ranura para candado tipo Kensington.

4.4.1.2 Características Mínimas específicas.

Las características recogidas en el presente capítulo son de obligado cumplimiento para la tecnología propuesta por el ofertante. El no cumplimiento de alguna de ellas, será motivo de exclusión de la propuesta presentada.

4.4.1.2.1 AP Básico.

- Punto de acceso básico 802.11ac Wave 2, con capacidad MU-MIMO/MIMO y con posibilidad de añadirles módulo para soportar *Bluetooth Low Energy* (BLE).
- 5GHz 3x3:3SS y 2,4GHz 2x2:2SS mínimo.
- 5GHz 3SS MU-MIMO mínimo.
- Soporte de canales adicionales de 5GHz que puedan ser liberados por las agencias FCC y ETSI.
- Al menos 1 puerto de red GbE.
- Alimentación *inline*. La universidad, comprometida con el ahorro energético, prefiere claramente que este tipo de equipos (AP Básicos) dado su gran número, soporten una alimentación basada en PoE (802.3af), sin perder o reducir ninguna de sus prestaciones de transmisión 80211ac. Es decir, se valorará especialmente un punto de acceso básico Wave 2 completamente funcional que no requiera obligatoriamente PoE+ (802.3at).
- Los puertos de datos y de alimentación deben estar orientados en paralelo a la tapa trasera y no en perpendicular.

4.4.1.2.2 AP Altas Prestaciones.

- Punto de acceso avanzado 802.11ac Wave 2, con capacidad MU-MIMO/MIMO y con posibilidad de añadirles módulo para soportar *Bluetooth Low Energy* (BLE).
- 5GHz 4x4:3SS y 2,4GHz 2x2:2SS mínimo.
- Soporte de VHT160.
- Soporte de canales adicionales de 5GHz que puedan ser liberados por las agencias FCC y ETSI.
- Dos interfaces Ethernet 100/1000 Mbps RJ-45.
- Al menos, uno de ellos, interfaz de red Ethernet con capacidad de 100/1000/2500 Mbps.
- Capacidad de establecer un enlace agregado con los dos interfaces mediante LACP.
- Capacidad de monitorización y optimización del consumo de potencia.
- Alimentación *inline* PoE o PoE+.
- Monitorización del espacio radioeléctrico para descubrimiento y gestión de interferencias y de *rogue* APs.

4.4.2 APs de exterior.

Se han suministrar e instalar APs de exterior con tecnología *mesh*.

El adjudicatario debe instalar, y conectar los APs de exterior en los sitios que se acuerden conjuntamente con los servicios técnicos de la universidad. Serán por cuenta del adjudicatario los soportes necesarios en cada caso.

Los ofertantes deben presentar un proyecto detallado de la instalación de APs de exterior.

4.4.2.1 *Características Mínimas*

Las características recogidas en el presente capítulo son de obligado cumplimiento para la tecnología propuesta por el ofertante. El no cumplimiento de alguna de ellas, será motivo de exclusión de la propuesta presentada.

- Certificado Wi-Fi Alliance (WFA) 802.11a/b/g/n/ac.
- *"Beamforming"* basado en estándares. Así como mantener la compatibilidad con estándares anteriores 802.11 a/b/g/n.
- Los APs deberán incluir tecnología MIMO con al menos soporte para 2 flujos espaciales.
- Las radios deberán poder hacer Análisis de Espectro para detectar interferencias no Wi-Fi y servir clientes de manera simultánea.
- Los APs deberán poder detectar y clasificar las fuentes de interferencia externas: Microondas, *bluetooth*, DECT, etc.
- Todos los APs ofertados deben incorporar radios de última generación con posibilidad de analizar el espectro con una resolución de 5Mhz, para detectar posibles interferencias.
- Soporte para protocolos de eficiencia energética, 802.3az, *Energy Efficient Ethernet*.
- Soporte de los siguientes métodos de cifrado:
  - CCMP/AES.
  - TKIP.
- Los APs deberán incluir filtros para protegerse de las interferencias provocadas por redes 3G/4G.
- Disponibilidad de diferentes soportes: para farolas, postes metálicos, voladizos, paredes, etc.
- Posibilidad de utilizar indistintamente la banda de 2,4GHz, o la de 5GHz, para formar la red de conexión entre los APs.
- Estanqueidad de los APs y las conexiones de los dipolos. Certificación mínima IP67.
- SU-MIMO 3x3:3SS o superior.
- IEEE 802.11ac.
- IEEE 802.11d.
- IEEE 802.11h.
- IEEE 802.11i.
- IEEE 802.11k.
- IEEE 802.11r.
- IEEE 802.11w.
- Soporte de hasta 16 SSID.
- Alimentación *inline* PoE o PoE+.
- Monitorización del espacio radioeléctrico para descubrimiento y gestión de interferencias y de *rogue points*.

4.4.3 Cantidades de Puntos de Acceso

4.4.3.1 *Puntos de Acceso de Interior*

Según la tabla de APs del Anexo III, en cualquier sitio donde existan APs diferentes del AP205, es instalación antigua con parámetros de cobertura del 2005. En esos sitios habrá que instalar nuevos APs y puntos de cableado, en nuevas localizaciones, en las proporciones que se estiman en el Anexo III.

Todos los APs retirados se entregarán a los servicios técnicos de la universidad.

Los APs se suministrarán e instalarán con el soporte habitual más sencillo de que dispone el fabricante para fijar en pared.

En la tabla del Anexo III se calcula que serían necesarios 1.442 APs. Este dato es orientativo.

A ello hay que sumar unos 58 APs para el edificio Trimodular que será incorporado a la red de la universidad durante la ejecución del proyecto descrito en este documento.

Además, para dar una mejor cobertura en zonas de alta densidad de usuarios, se piden 50 APs de Altas Prestaciones.

Por tanto, y de acuerdo con el proyecto piloto, se estima que se han de suministrar e instalar mil quinientos APs básicos y cincuenta APs de altas prestaciones.

4.4.3.2 Sustitución de APs del proyecto piloto.

En este apartado, se detalla lo que es necesario hacer si todos los APs del proyecto piloto, y los APs Wave 1 del Colegio Mayor, actualmente instalados, no pueden ser plenamente incorporados y gestionados por la nueva infraestructura que se oferte.

Si fuese este el caso, hay que suministrar ciento cincuenta y un APs Básicos adicionales SIN instalación de cableado. 121 por el proyecto piloto y 30 por el Colegio Mayor.

En la Facultad de Derecho y los módulos de Ciencias del proyecto piloto, no hay que realizar estudios de cobertura inicial ni final, ni instalación de cableado. Solo hay que sustituir los ciento veintiún APs de Alcatel actuales por ciento veintiún APs Básicos ofertados en este apartado.

En el Colegio Mayor si hay que realizar estudios de cobertura inicial y final en todo el edificio. En este edificio hay que realizar dos tareas:

- Sustituir los 30 AP205 Wave 1 actuales por 30 APs Básicos.
- Sustituir los AP70 actuales con los APs estimados en el Anexo III, y completar la cobertura por todo el edificio.

4.4.3.3 Exterior

Se han suministrar e instalar veintisiete APs de exterior con tecnología *mesh*.

Doce de ellos estarán conectados y alimentados a través de una roseta de cableado utp Cat6A como las descritas en este documento, con la única diferencia de utilizar cable utp de exterior. Estarán situados en paredes, voladizos y techos de edificios.

Los otros quince restantes estarán conectados por medio de tecnología *mesh*, y se requiere que el adjudicatario los instale en farolas, postes de pistas deportivas o cualquier otro sitio que el estudio inicial de cobertura considere oportuno.

Se realizará estudio de cobertura final para verificar que se obtienen los resultados esperados.

4.5 Líneas eléctricas de exterior.

El adjudicatario debe realizar la conexión eléctrica de los quince APs de exterior de la forma que se indica a continuación.

- Realizada en con conductor de cobre flexible, respetando como mínimo la sección de 2,5mm^2 para los conductores activos. Será obligatorio que cada circuito eléctrico cuente con el hilo de puesta a tierra con independencia de que el propio AP lo necesite o no. En circuitos interiores de edificios será libre de halógenos, discurriendo bajo tubo flexible corrugado de PVC también libre de halógenos. El tubo estará fijado por medios mecánicos cada metro. Los circuitos exteriores a edificios se tenderán bajo tubo metálico enchufable y cajas IP 65 con entrada a racord. Se instalarán cajas de registro de medidas adecuadas cada 25 metros y en ellas se dejará una pequeña coca de cable. En cada uno de los extremos de la línea se rotulará la denominación de esta (ejemplo LINEA WIFI Nº5), con esta misma denominación se rotularán las tapas de las cajas de registro.
- Se instalará y conexionará como protección eléctrica de cada circuito de alimentación, una protección iDPN Vigi 2x16A, 30mA SI, ubicándolo en el armario eléctrico más cercano.
- En el otro extremo de la línea, y próximo al propio AP, se instalará un dispositivo de corte omnipolar, Vario DE SCHNEIDER de 16 A, ref. VCF01GE. Estará rotulado con la denominación del circuito eléctrico y el cuadro eléctrico que lo alimenta
- El montaje se hará cumpliendo el REBT y será realizado por un instalador autorizado. Hay que presentar el documento que lo acredite a los servicios técnicos de la universidad antes de realizar la instalación.

4.6 Conmutadores de acceso.

La empresa debe suministrar, instalar y configurar, los suficientes conmutadores PoE/PoE+ con todas las bocas 100/1000 necesarias para activar todos los APs en 802.11ac Wave 2 de cada armario. No hay que sustituir las pilas actuales que dan servicio a ordenadores de usuarios y teléfonos IP.

Los nuevos conmutadores serán los conmutadores de cabecera de cada armario, conectándose a 1Gb o 10Gb al armario de agregación superior, y darán paso a la pila de conmutadores con la que ahora mismo se da servicio a los usuarios.

Por tanto, el adjudicatario debe configurar los nuevos equipos para mantener todos los parámetros de la infraestructura actual: VLANES, DHCP Snooping, ACLs, QoS, VoIP, 802.1X, etc.

En el apartado "Cantidad de conmutadores" se indica el equipamiento a suministrar, tanto si los conmutadores nuevos soportan los SFPs de los conmutadores actuales, como si no los soportan.

La instalación de los nuevos conmutadores, y la conexión entre los nuevos y los viejos, la realizará el integrador con latiguillos RJ-45<->RJ-45 y varios enlaces LACP, bajo la supervisión de los servicios técnicos de la universidad.

4.6.1 Especificaciones técnicas mínimas de los conmutadores.

Cada uno de estos equipos, además de proporcionar la conectividad suficiente para los requisitos solicitados, deberá cumplir estas características:

- Serán equipos de enracables en armarios de 19".
- Alimentación *inline*.
    - Podrán disponer de 24 o 48 puertos 100/1000 Base-T PoE/PoE+, pero siempre suministrarán la alimentación PoE y PoE+ necesaria a los puntos de acceso ofertados que se conecten al conmutador, de forma que todos los APs ofrezcan simultáneamente funcionalidad completa 802.11ac Wave2.

- Si los APs Básicos ofertados son alimentados con PoE+, los conmutadores deben suministrar PoE+ suficientes en sus bocas.
- Si los APs Básicos ofertados son completamente funcionales Wave 2 con PoE, los conmutadores que se propongan deben suministrar mayoritariamente bocas PoE, pero deben permitir algunas bocas PoE+ para dar servicio a los APs de Altas Prestaciones y de Exterior, que podrían situarse en cualquier armario de comunicaciones.

- Dispondrá de al menos 4 puertos SFP+ de 1/10G, admitiendo conectores de velocidades 1/10Gbps.
- Equipo *Non-Blocking*: La capacidad de conmutación debe ser mayor o igual que la suma de ancho de banda de todos los puertos, considerando ambos sentidos. Con la configuración mínima solicitada, 128Gbps para el equipo de 24 puertos, y 176Gbps para el de 48 puertos. Dispondrá de puerto consola o serie para administración fuera de banda.
- Auto-configuración de puertos para APs. El dispositivo debe ser capaz de detectar y autoconfigurar un AP dinámicamente y aplicarle una política predefinida en el equipo, únicamente en los puertos que haya detectado un AP. Deben soportarse los APs que se oferten en respuesta a este pliego.
- Deberá soportar la programación via Openflow, de redirección de flujos de tráfico a túneles GRE.
- Protocolos de Spanning-Tree: IEEE 802.1s Multiple Instance Spanning Tree.
- Soportará sFlow, RFC 3176 y/o NetFlow v9, RFC 3954.
- Soportará Openflow 1.3, directamente por el equipo, sin necesidad de que ninguna estación intermedia haga de proxy.
- Soporte de QoS.
- Portal cautivo. Posibilidad de autenticar usuarios contra el portal cautivo que se use en la plataforma inalámbrica.
- Facilidades de despliegue. Con el objeto de optimizar el tiempo empleado por parte de los trabajadores del departamento de TI de la Universidad, se necesita que los conmutadores tengan una serie de características que permitan la rápida y sencilla reubicación y reinstalación de dichos dispositivos en cualquier entorno de la Universidad. Dichas características son:
  - Botón de reseteo del equipo. Permite llevar el equipo a configuración de fábrica.
  - Soporte de despliegues tipo *Smart Install*. Se requiere que el equipo pueda ser desplegado, simplemente sacándolo de la caja y enchufándolo en la red. En coordinación con la plataforma de gestión, recibirá la configuración prevista.
- Posibilidad de presentar portal cautivo para invitados o usuarios no autenticados.
- Soporte de roles de usuario que permitan diferenciar el tráfico de los usuarios y los destinos permitidos sin necesidad de separarlos en VLANs según para cada tipo de servicio prestado. Se soportarán las siguientes funcionalidades:
  - Asignación de límites de ancho de banda
  - Reglas de control de acceso basadas en la identidad del usuario y no en la dirección del origen del usuario
  - VLAN asociada al tipo de usuario
  - Reglas de calidad de servicio asociadas al tipo de usuario
- Los equipos deben soportar Trust QoS. Deben permitir la autoconfiguración de QoS cuando se conecte un AP.
- El equipo debe poder configurarse por consola pero mediante un menú interactivo, sin necesidad de conocer comandos. Esta opción se solicita para disminuir los requisitos que deben tener los operadores para mantener la red.

4.6.2 Cantidad de conmutadores.

Basada en la experiencia de la universidad con el proyecto piloto, en la tabla del Anexo III se indica en la columna "Previsiones de APs Básicos nuevos a instalar", el número de APs Básicos que es previsible que se instalen en cada armario de comunicaciones de la universidad.

En la columna "Puertos PoE mínimos a instalar", se indica el número de puertos PoE simultáneos que deben alimentar, como mínimo, los conmutadores que proponga el ofertante en cada armario. Con ello, la universidad quiere que el ofertante, no sólo suministre los conmutadores necesarios para los APs Básicos estimados, sino que se puedan alimentar algún AP adicional, PoE o PoE+, por las siguientes razones:

- Los estudios de cobertura podrían añadir algún AP Básico (PoE) a los estimados.
- Alguna de las dependencias cubiertas por el armario requiere un AP de Altas Prestaciones (PoE+).
- Algún AP de Exterior (PoE+) ha de alimentarse desde ese armario.

Ahora bien, si todos los APs ofertados requieren PoE+ para ser completamente funcionales en 802.11ac, los conmutadores ofertados en cada armario de comunicaciones deben proporcionar puertos PoE+ en el número que aparece en la casilla "Puertos PoE mínimos a instalar".

Además de los conmutadores, el adjudicatario debe suministrar SFP+ y latiguillos. En este apartado hay dos escenarios posibles.

4.6.2.1 SFPs y SFP+s actualmente en uso reutilizables.

Si los conmutadores propuestos para satisfacer este pliego, soportan la reutilización de los SFPs y SFPs+ que están funcionando ahora mismo en los conmutadores de acceso Cisco actuales, el licitador debe suministrar:

- 45 SFP+ 10GBase-LR.
- 50 latiguillos bi-fibra monomodo 3mts LC-SC con cubierta de color amarillo.
- 160 latiguillos estándar, NO cruzados, RJ-45<->RJ-45 Cat6A de 1,5 metros.

4.6.2.2 SFPs y SFP+s actualmente en uso NO reutilizables.

Si los conmutadores propuestos para satisfacer este pliego, NO soportan la reutilización de los SFPs y SFPs+ que están funcionando ahora mismo en los conmutadores de acceso Cisco actuales, el licitador debe suministrar:

- 50 SFP+ 10GBase-LR.
- 170 SFP 1GBase-LR.
- 50 latiguillos bi-fibra monomodo 3mts LC-SC con cubierta de color amarillo.
- 160 latiguillos estándar, NO cruzados, RJ-45<->RJ-45 Cat6A de 1,5 metros.

4.7 Plataforma de gestión.

La universidad quiere mejorar sustancialmente la plataforma de gestión de equipos que tiene actualmente. Para ello requiere que la nueva plataforma que se oferte sea capaz de gestionar, de la forma más completa posible, tanto los equipos ofertados objeto de este pliego, como los equipos existentes ahora que no van a ser sustituidos.

La universidad puede incorporar, en el futuro, equipamiento de red otros fabricantes no citados en este documento. Por tanto, el soporte multifabricante de la plataforma de gestión ofertada debe ser lo más amplio posible.

La universidad dispone actualmente de un Cisco Prime Infraestructure 2.0, con licencia para 300 nodos. Está instalado en la plataforma de virtualización VMware de la universidad descrita en el Anexo I. El uso actual de esta herramienta se reduce a repositorio de configuraciones. Sin embargo se pretende utilizar todas las funcionalidades que la herramienta ofrece.

El adjudicatario deberá actualizar dicha herramienta o bien sustituirla por una nueva para cumplir todos los requerimientos que se mencionan en este apartado.

El actual Omnivista 3600 de Alcatel (Airwave de Aruba), puede gestionar dispositivos de otros fabricantes. La licitante puede ampliar las licencias de Omnivista para que gestione todos los componentes del nuevo sistema, o proponer otro sistema de gestión y elaboración de informes, completamente diferente, que cumpla las mismas funcionalidades o superiores, que actualmente proporciona el Omnivista/Airwave.

El adjudicatario debe realizar los trabajos necesarios para situar todos los nuevos APs en los planos del Omnivista, o en la herramienta de gestión sustituta.

El adjudicatario debe realizar todos los trabajos necesarios para que toda la electrónica de la universidad, tanto los nuevos equipos objeto de este pliego, como la antigua electrónica que permanezca, quede integrada en la plataforma ofertada.

Si la plataforma ofertada es completamente nueva, y no una actualización del Prime u Omnivista, además de las licencias necesarias para gestionar el equipamiento ofertado, se han de incluir las licencias necesarias para que la plataforma ofertada gestione los conmutadores actualmente en uso en la universidad: quinientos conmutadores agrupados en ciento cincuenta pilas.

En el caso de los conmutadores, las herramientas de gestión englobarán tanto a los nuevos conmutadores como a los actuales conmutadores Cisco. El adjudicatario realizará los ajustes necesarios para aplicar las siguientes funcionalidades a todos ellos:

- Despliegue de configuraciones de forma centralizada en base a plantillas desde las herramientas de gestión.
- Provisionamiento de nuevos conmutadores en la red.
- Configuración centralizada de VLANES y despliegue en puertos de acceso y de *trunk*.
- Mecanismos automáticos de detección de desviación de las configuraciones respecto a la configuración validada.
- Repositorio de configuraciones con un histórico de 1 año.
- Despliegue de cambios de versión de firmware.
- Mecanismos automáticos de detección de desviación de las versiones de firmware respecto a la versión validada.

Una vez finalizada la integración de todos los conmutadores en las herramientas de gestión, el adjudicatario deberá demostrar que los requerimientos exigidos se cumplen en los conmutadores nuevos y en los actuales.

El adjudicatario entregará una documentación con los procedimientos detallados de aplicación de las funcionalidades que se han detallado en la lista anterior, que incluirá también las necesidades de mantenimiento de las herramientas de gestión.

4.7.1 Características Mínimas.

Las características recogidas en el presente capítulo son de obligado cumplimiento para la tecnología propuesta por el ofertante. El no cumplimiento de alguna de ellas, será motivo de exclusión de la propuesta presentada.

- Soporte de la plataforma:
  - El adjudicatario debe suministrar, instalar y configurar un *appliance* físico o bien suministrar una licencia sobre máquina virtual que se alojará en la plataforma de virtualización VMware de la universidad antes descrita, pero deberá indicar los requerimientos, tanto *hardware* como *software*, para poder usar dicha plataforma cubriendo todas las necesidades de este proyecto.
  - La plataforma de gestión debe proporcionar licenciamiento suficiente para gestionar los equipos de este proyecto, los conmutadores de CORE, distribución y acceso, actualmente instalados en la red de la universidad.
- Dispositivos:
  - Auto-Descubrimiento de dispositivos.
  - Descubrir automáticamente nuevos elementos de red que se vayan incorporando.
  - La plataforma debe ser multifabricante.
  - La plataforma debe permitir la gestión, (fallos, gestión de configuraciones, inventario y recepción de alarmas), para los fabricantes instalados en la universidad (Cisco Catalyst, Cisco Nexus y Alcatel-Aruba), y para la electrónica que sea propuesta por el licitante.
- Operación:
  - La plataforma de gestión debe poder operarse mediante interfaz HTML con protocolo de acceso HTTPS a todos los módulos, además de:
    - Acceso a consola e interfaz de comandos (CLI).
    - Acceso remoto a consola mediante *Secure Shell* (SSH).
  - Actualización y reinicio programable de dispositivos.
- Monitorización:
  - Permitirá su integración con sistemas de gestión mediante SNMP.
  - Permitirá la notificación y seguimiento de fallos a través de notificaciones en distintos formatos (Syslog, *e-mail* y SNMP *Traps*).
  - Permitirá la supervisión y control de toda la infraestructura inalámbrica, mediante la recolección de alarmas y eventos de los elementos de la misma, y su representación visual.
  - Permitirá monitorizar los conmutadores a los que están conectados los APs, facilitando información sobre disponibilidad y utilización de los puertos, CPU, y memoria.
  - Permitirá la configuración y administración completa de todos los elementos de la red inalámbrica.
  - Monitorización de todos los APs, controladoras, clientes y de los conmutadores que tengan conectados APs.
  - Almacenamiento de la calidad y los problemas de las conexiones realizadas en el último mes.
  - Monitorización y reporte de los posibles problemas de conexión de los clientes.
  - Identificar tipos y características de dispositivos conectados.
  - Identificar tipos de tráfico y aplicaciones utilizadas.
  - Monitorización de uso en tiempo real. Se debe poder monitorizar en vivo el comportamiento de los clientes y visualizar el comportamiento de la

asociación radio de los clientes, la autenticación, el servicio DHCP y DNS, así como las tasas de fallos.

- Alertas y diagnósticos:
  - Permitirá funcionalidades de ajuste de umbrales para la generación de eventos y alarmas en base a diferentes criterios.
- Capturas de tráfico:
  - La plataforma debe permitir la definición de sesiones de captura de tráfico pudiendo seleccionarse, todos o un subconjunto de:
    - Protocolo TCP/UDP
    - IP Origen
    - IP Destino
    - MAC Origen
    - MAC Destino
  - Se podrán definir varias capturas.
  - Debe ser posible la activación de la captura de forma remota, sin necesidad de conectarse al equipo, y sin degradación del rendimiento ofrecido al usuario final.
  - Debe poder monitorizarse en tiempo real la captura.
  - Desde la consola HTML, debe ser posible la descarga en formato PCAP, para ser abierto por aplicaciones como Wireshark.
  - No debe requerir condiciones especiales a la conectividad (VLANs, SPANs, o similares). Debe ser posible la activación en equipos remotos, con los que se tenga conectividad de gestión con la IP de gestión, a través de redes L2 o L3, así como equipos que pudieran estar fuera del campus pero que estén administrados desde la plataforma.
- Gestión de la configuración:
  - Auto-Configuración de los APs que se vayan incorporando a la red.
  - Permitirá la creación de grupos de dispositivos en función de distintos criterios definidos por el administrador. Estos grupos pueden tener una organización jerárquica o definir macrogrupos seleccionando múltiples grupos.
  - Configuración masiva de dispositivos mediante la descarga de plantillas que se cargan simultáneamente a grupos de APs creados por el administrador.
  - Facilitará la creación y monitorización de WLANs.
  - Permitirá almacenar, al menos, el último fichero de configuración, facilitando la "marcha atrás" en caso de ser necesario.
  - Archivo, descarga y copia de configuraciones.
- Gestión de políticas y auditorías:
  - Comprobación de las políticas de seguridad configuradas en los APs, detectando violaciones o deficiencias en la configuración del SSID, *broadcasts*, 802.1X o WEP.
- Gestión y distribución de *Firmware*:
  - Actualización centralizada del *firmware* de los dispositivos. Esta tarea podrá realizarse automáticamente de forma programada, o mediante actuaciones puntuales.
  - Detección de equipamiento con versiones de *software* no actualizadas, y distribución de las actualizaciones a todos los equipamientos que lo necesiten.
- Visualización y servicios de localización:
  - El sistema debe disponer de un sistema de localización y seguimiento en tiempo real y tridimensional. En tiempo real porque el sistema debe ir actualizando en tiempo real la posición del elemento a seguir. Tridimensional porque debe tener en cuenta los APs de todas las plantas para la localización del equipo.

- El sistema debe proporcionar estudios de cobertura en tiempo real. Debe mostrar los mapas de color, con la distribución de frecuencias y potencias, en tiempo real, a partir de la información que capturan todos los APs.
- Soportará la funcionalidad de mapa de red en donde se presente el estado de todos los elementos de la red inalámbrica, así como su estado de operación con tiempos de refresco no superiores a 5 minutos. Esto debe incluir la representación, al menos, de los siguientes elementos:
  - Estado operativo de los elementos de la red inalámbrica.
  - Representación del estado de cobertura de toda la red en cada centro. Se deberá reportar y resaltar visualmente cualquier zona sin cobertura (zona oscura).
- Situar todos los APs de la red utilizando planos procedentes de ficheros dwg.
- Mostrar parámetros de cobertura por medio de "mapas de calor".

- APs *Rogues* y detección de intrusión:
  - Permitirá la detección de APs instalados sin autorización (*Rogue Access Points*), que son instalados sin el control por parte de los servicios técnicos de la universidad, generalmente para el acceso sin autorización a la red y los sistemas de información.
  - Monitorizará el espectro radioeléctrico para detectar posibles interferencias, así como situaciones en las cuales la calidad del servicio está sufriendo degradaciones. También tiene que permitir ver los diagramas de radiación que se están produciendo, y detectar la existencia de posibles zonas de sombra.
- Soporte para planificación de red y despliegue. Dispondrá de una herramienta que permita estimar y planificar el despliegue de nuevos APs. Esto se realizará en planos ya definidos en la plataforma en los que ya se hayan definido APs instalados. De esta forma, la universidad podrá decidir la mejor ubicación para las ampliaciones de APs.
- Informes:
  - Realización de informes a demanda y automatizados, en periodos de tiempo seleccionables, sobre toda la red o sobre grupos de APs:
    - de los APs más utilizados o con más usuarios,
    - de usuarios y dispositivos con más sesiones y con más tráfico,
    - de tipos y fabricantes de dispositivos conectados,
    - de aplicaciones y tipos de tráfico que atraviesan la red inalámbrica.

4.8 Servidor de AAA (*Authentication, Autorization & Accounting*).

La universidad considera que es necesario cambiar del *software* AAA actual, FreeRADIUS, por otro que proporcione una mayor flexibilidad, y del que el adjudicatario pueda dar un buen soporte.

Esta es la pieza esencial que podrá facilitar un despliegue unificado de 802.1X en todos los entornos de red de la universidad. Los perfiles y permisos se aginarán a los roles y los usuarios de igual forma en la red inalámbrica y en los conmutadores suministrados.

La universidad considera que, para una gestión y control más unificado, lo más recomendable sería que algunos componentes que ahora están separados, estuviesen unidos en un entorno común: AAA, *accounting*, portal de invitados, etc. Aunque, si se cumplen las especificaciones de este documento, la universidad puede aceptar que los ofertantes presenten herramientas específicas, en vez de unificadas.

El adjudicatario debe realizar todos los trabajos necesarios, tanto en el *software* que proponga en este apartado, como en el resto del equipamiento ofertado, controladoras, conmutadores,

plataforma de gestión, etc., para que todo el conjunto quede listo para su uso por parte de los servicios técnicos de la universidad.

Actualmente, la universidad dispone de equipamiento, inalámbrico y cableado, que utiliza el *software* AAA del que dispone actualmente, el FreeRADIUS. Parte de ese equipamiento se dará de baja tras la instalación de la red inalámbrica objeto de este pliego.

El adjudicatario debe configurar también, el *software* AAA que suministre, para que funcione con el equipamiento que permanezca en la universidad, conmutadores antiguos, servidor vpn, *firewalls*, etc. Sin embargo, la configuración de los equipos no afectados por este pliego, que requieren el uso del *software* AAA, la harán los servicios técnicos de la universidad.

4.8.1 Características Mínimas Generales.

Las características recogidas en el presente capítulo son de obligado cumplimiento para la tecnología propuesta por el ofertante. El no cumplimiento de alguna de ellas, será motivo de exclusión de la propuesta presentada.

- Es obligatorio el suministro, instalación y configuración en *appliance* físico.
- Se han de instalar, configurar y mantener, al menos, dos instancias del *software*.
- Se considera incluida cualquier licencia o coste adicional necesario para mantener la alta disponibilidad en dicho sistema. Estos *appliances* serán gestionados desde la plataforma de gestión ofertada.
- El sistema completo debe ser capaz de soportar al menos cincuenta mil direcciones (50.000) MAC diferentes a la semana.
- El sistema completo debe tener capacidad para realizar un mínimo de doscientas cincuenta (250) autenticaciones por segundo.
- El sistema será suministrado con las licencias necesarias para soportar durante toda la vigencia del contrato, al menos veinticinco mil (25.000) dispositivos concurrentes en alta disponibilidad.
- El sistema de gestión de políticas de Seguridad deberá utilizar protocolos estándar que garanticen su compatibilidad con distintos equipos de acceso (conmutadores, enrutadores, *firewalls*, controladores WLAN, terminadores VPN) de los principales fabricantes presentes en la Universidad: Cisco, Alcatel-Aruba, Palo Alto Networks, FreeRADIUS.
- El sistema debe validar, también, credenciales registradas en fichero plano o en una base de datos local. Ahora mismo, la universidad proporciona acceso por VPN a técnicos de diferentes empresas para realizar mantenimiento. El RADIUS actual, ante una petición de autenticación del servidor de VPN, chequea en primer lugar el fichero donde están registrados esos usuarios externos. Si las credenciales no están en ese fichero, el RADIUS actual busca esas credenciales en el LDAP corporativo de la universidad. El RADIUS actual es el que indica el grupo de usuarios al servidor de VPN.
- El *software* AAA debe tener entornos de administración diferenciados. El operador de red inalámbrica debe poder configurar todo lo que necesite sin que ello afecte a la red cableada, servicios de VPN u otros adicionales. De igual forma, el operador de red cableada debe poder configurar todo lo que necesite sin que ello afecte a la red inalámbrica y el resto de servicios. Lo mismo es aplicable a otros entornos: VPN, *firewalls*, test, etc. La idea principal es que, ya que cada entorno es administrado por técnicos diferentes, las acciones que cada técnico realice en el *software* AAA para administrar su propio entorno no cambie la configuración del resto.
- Los perfiles de usuario y grupo deben poder deducirse de propiedades de los usuarios almacenadas en el directorio LDAP corporativo de la universidad. Estos perfiles deben

poder ser utilizados por todos los entornos administrativos mencionados en el punto anterior.

- Debe tener Entidad Certificadora integrada, pudiendo usarse en ausencia de otra externa. Los certificados de esa Entidad podrán ser usados para la autenticación de dispositivos asociados.
- El sistema deberá tener la capacidad (y tenerla activa durante todo el ciclo de vida del proyecto) de identificación de los dispositivos conectados a la red para aplicar políticas en función del tipo de dispositivo.
- Se deberá poder utilizar mecanismos como:
    - MAC OUI.
    - Huella DHCP.
    - HTTP *User Agent*.
    - Escaneos de puertos.
    - Escaneos SNMP.
    - Agente NAC.
    - *Onboarding*.
- Soporte de servicios AAA (*Authentication, Authorization* y *Accounting*) de red con los métodos de autenticación más utilizados en la industria:
    - RADIUS, RADIUS CoA.
    - EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS).
    - PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS).
    - TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP).
    - EAP-TLS.
    - PAP, CHAP, MSCHAPv1 y 2, EAP-MD5.
    - Autenticación de máquina en dominios Windows.
    - MAC auth (non 802.1X devices).
    - Autenticación Web (Portal Cautivo).
- Posibilidad de separar los procesos de Autenticación y Autorización. Cada proceso deberá poder utilizar bases de datos distintas.
- El sistema deberá soportar, y tenerla activa durante todo el ciclo de vida del proyecto, integración bidireccional con el *firewall* desplegado actualmente en la red (Palo Alto Networks). El sistema de control de acceso enviará al *firewall* la información de usuario, dispositivo, salud, etc., asociada a cada IP. El sistema de control de acceso deberá poder recibir del *firewall* eventos de seguridad y tratarlos para modificar el acceso a la red de los dispositivos afectados.
- El sistema deberá poder integrarse con el servicio Eduroam desplegado en la universidad. Para ello tendrá que poder hacer "Proxy RADIUS" hacia los servidores AAA de RedIRIS así como recibir autenticaciones del RADIUS de RedIRIS. También debe hacer de "Proxy RADIUS", en entrada y salida, para otras organizaciones alojadas bajo el dominio de la UAM (*.uam.es) y que hacen uso de la iniciativa Eduroam.
- Compatibilidad con distintas bases de datos:
    - Microsoft Active Directory.
    - Kerberos.
    - LDAP estándar.
    - SQL.
    - ODBC.
- El sistema implementará los siguientes estándares RFC:
    - RFC 2246 The TLS Protocol Version 1.0.
    - RFC 2248 Network Services Monitoring MIB.
    - RFC2548 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 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 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs.
- RFC 4137 State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator.
- RFC 4849 RADIUS Filter Rule Attribute.
- RFC 5216 The EAP-TLS Authentication Protocol.

- La solución aportada debe poder integrarse con distintos tipos de autenticación de doble factor (2FA), y como mínimo, debe soportarse y configurarse por el ofertante una autenticación en la entrega, en la que el teléfono móvil sea usado como *token*.
- Debe tener APIs para poder realizar integración con sistemas externos.

4.8.2 Características Mínimas Control de acceso de invitados.

Las características recogidas en el presente capítulo son de obligado cumplimiento para la tecnología propuesta por el ofertante. El no cumplimiento de alguna de ellas, será motivo de exclusión de la propuesta presentada.

- El sistema incluirá un portal cautivo para la autenticación de invitados compatible con cualquier solución WLAN.
- El sistema deberá permitir varios portales cautivos, pudiendo usarse simultáneamente bajo diversas condiciones, como por ejemplo, diversos SSIDs, medio cableado o medio inalámbrico, entorno corporativo o entorno de invitados.
- El tiempo de expiración de las cuentas de invitados deberá ser configurable.
- El sistema deberá tener capacidad para cachear la sesión de un usuario, evitando así que reaparezca el portal de invitados ante una suspensión del dispositivo cliente.
- El portal cautivo incluirá funcionalidades avanzadas de auto-registro, mediante las cuales el invitado podrá generar su propia cuenta de invitado sin comprometer la seguridad de la red.
- El portal proporcionará diversos métodos para la entrega de credenciales de invitado: e-mail, SMS, impresión de tickets.
- El portal proporcionará métodos avanzados de aprobación de la visita por parte de la persona que recibe al invitado que permitan autorizar la visita de manera flexible y sin intervención de personal de tecnologías.
- El sistema deberá poder actuar como Service Provider (SP) de SAML[2], pudiendo llegar a integrarse el uso de las credenciales de red, con aplicaciones que usen este método de autenticación.
- El sistema debe poder validar a los usuarios contra el directorio LDAP corporativo de la universidad.
- El portal proporcionará informes de actividad relativa al tráfico de invitados: número de visitas, contenido multimedia mostrado, numero de SMS enviados con credenciales, numero de e-mails enviados, etc.
- Se deben poder seleccionar usuarios específicos para administrar los portales de invitados diferentes a los administradores de la aplicación completa.

[2] https://es.wikipedia.org/wiki/Security_Assertion_Markup_Language

- Se requiere la posibilidad de autenticar a los usuarios invitados validarse con sus credenciales en las redes sociales más utilizadas en España, según el último estudio publicado por el Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (ONTSI):
    - Facebook.
    - Google.
    - Twitter.
- Requisitos de personalización del portal de invitados:
    - Inclusión en el portal de menús desplegables que permitan registrar información relativa al invitado: motivo de la visita, duración de la misma, persona a la que visita, etc.
    - Integración con "PassBook" (iOS) o "PassWallet" (Android, W8) para facilitar la distribución de agendas en eventos o galas.
    - Generación de portales HTML de distinto tamaño en función del tamaño y resolución de las pantallas de los dispositivos móviles.
    - Posibilidad de incluir todo de tipo de contenido multimedia en el portal: imágenes, audio, video, etc., que varíe de forma dinámica según patrones establecidos.
- La plataforma de gestión de acceso dispondrá de una CA integrada para generar certificados digitales que garanticen el acceso seguro a la red de los dispositivos móviles.
- Control de acceso a la red y también de aplicaciones:
    - El sistema deberá poder actuar como Identity Provider (IdP) de SAML.
    - El sistema deberá poder actuar como Service Provider (SP) de SAML.
- La solución de control de acceso deberá poder integrarse con los fabricantes de *firewall* más utilizados, particularmente con Palo Alto Networks. Entendemos por integración disponer de manera nativa de la capacidad del intercambio de parámetros de movilidad (*username*, *device-type*). Estos parámetros permitirán al *firewall* aplicar unas políticas más granulares, redundando en una mayor seguridad global.
- La solución ofertada debe poder ser utilizada desde conmutadores y redes inalámbricas de otros fabricantes no mencionados en este documento.

4.8.3 Características Mínimas Provisión Automática de Dispositivos.

Las características recogidas en el presente capítulo son de obligado cumplimiento para la tecnología propuesta por el ofertante. El no cumplimiento de alguna de ellas, será motivo de exclusión de la propuesta presentada.

- La provisión de dispositivos móviles deberá ser un proceso automatizado que no implique una carga para los servicios técnicos de la universidad. El sistema deberá permitir la generación automática de certificados que se instalen en los dispositivos móviles, y permitan ser revocados ante la pérdida o robo de dicho dispositivo móvil.
- La conexión de los dispositivos móviles provisionados deberá hacerse utilizando EAP-TLS.
- El sistema proporcionará una infraestructura PKI interna que permita generar credenciales específicas para dispositivos móviles que sirvan para autorizar estos dispositivos en la red mediante certificados X.509.
- El sistema deberá ser capaz de avisar a los usuarios de la cercanía de la fecha de expiración de los certificados generados.
- Dispondrá de un portal de auto-servicio que permita a los usuarios gestionar (revocar, deshabilitar temporalmente, acceso impresoras en red, etc.) sus dispositivos móviles.
- El sistema de provisión automatizada debe ser compatible con los dispositivos más habituales:

    - Smartphones: iOS y Android
    - Laptops: MacOS X, Windows XP, Windows 7, Windows 8 y Windows 10.
- El sistema deberá configurar de manera automática el suplicante 802.1X de los dispositivos móviles.
- El sistema debe poder configurar de manera automática los parámetros de uso habituales en el entorno de trabajo: servidor de correo, cliente VPN, etc.
- El sistema proporcionará estadísticas de uso e inventario de los dispositivos móviles.
- La solución ofertada debe poder ser utilizada desde conmutadores y redes inalámbricas de otros fabricantes no mencionados en este documento.

4.8.4 Características Mínimas *Accounting.*

- Los registros de conexiones de usuarios se deben poder almacenar por lo menos durante dos años.
- Se necesita que, por cada sesión inalámbrica, de VPN, de 802.1X en red cableada, etc., se almacenen, al menos, los siguientes datos:
    - AcctSessionId: Identificador único de sesión.
    - UserName: Identificador de usuario.
    - AcctStartTime, AcctStopTime: Hora de comienzo y final de la sesión.
    - CallerStationId: Dirección MAC en la red inalámbrica y 802.1X cableada, dirección IP en VPN.
    - FramedIPAddress: Dirección IP asignada a la sesión.
    - NASIPAddress: Dirección IP del NAS o equipo de acceso sobre el que se ha solicitado la validación: controladoras, VPN, conmutadores, etc.
    - SSID.
    - VLAN.
- Son aceptadas una de estas dos soluciones:
    - Que la plataforma almacene los registros localmente.
    - Que la plataforma exporte vía *syslog* a un colector externo.
- El ofertante debe indicar con toda claridad si almacena los registros en la plataforma que oferta siguiendo este documento, o bien, si los exporta vía *syslog* a una plataforma externa.
- En el caso que almacene los registros en la plataforma ofertada, deberá indicar de qué forma y con qué tareas, conseguirán sus técnicos el almacenamiento de estos datos.
- El ofertante debe asegurar que el almacenamiento y tratamiento de estos datos de *accounting* en la plataforma ofertada no producen merma, ni en el rendimiento, ni en la capacidad de esos componentes, para realizar sus tareas principales.
- Si el almacenamiento y tratamiento de estos datos de *accounting*, producen merma en el rendimiento, o en la capacidad, de esos componentes, para realizar sus tareas principales, el ofertante debe proponer una solución alternativa.
- Si la solución alternativa requiere de alguna máquina virtual, ésta se alojará en la plataforma de virtualización VMware de la universidad antes descrita.
- Si la solución alternativa requiere máquina virtual, pero el aplicativo que suministre y configure el adjudicatario, no incluye el sistema operativo, la universidad podrá poner y mantener Windows o Linux. La universidad prefiere poner Red Hat siempre que pueda. El adjudicatario configurará el software que proporcione.
- El ofertante debe indicar las especificaciones de la máquina virtual necesaria, si fuese el caso.
- Si se utiliza una plataforma externa a la que se exporten los mensajes de *syslog*, se han de instalar, configurar y mantener, al menos, dos instancias del software para asegurar la alta disponibilidad.

4.9 Cableado.

Por cada nueva localización donde se vaya a montar un AP hay que instalar dos cables Cat 6A, con su correspondiente caja de superficie, desde el armario de comunicaciones que corresponda.

La empresa adjudicataria debe suministrar e instalar todos los componentes necesarios para la instalación del cableado: paneles, pasahilos, bloques de conexión, módulos, tubo corrugado, canaleta pequeña, etc.

Con respecto a los paneles hay varias condiciones a tener en cuenta.

- El instalador debe aprovechar los paneles de cableado a medio ocupar ya existentes en los armarios. La universidad no quiere tener huecos sin ocupar en los paneles de cableado.
- La gran mayoría de los armarios de comunicaciones, el 70% aproximadamente, están instalados con tecnología 110. En esos sitios, la instalación del nuevo cableado se hará sobre paneles 110. **La universidad suministrará los paneles metálicos de 4Us, paneles 110 sin patas y pasahilos 110 que se necesiten**. El instalador debe suministrar y engastar los bloques de conexión 110 de cuatro pares, con una herramienta de impacto 110 de cuatro o cinco pares adecuada. También se deben suministrar porta-etiquetas transparentes para paneles 110.
- Aunque sea una tecnología antigua, es obligatorio que la empresa ofertante tenga experiencia en el manejo de componentes 110.
- Allí donde haya paneles RJ-45, el instalador debe suministrar e instalar todos los paneles RJ-45, módulos y componentes que se necesiten. Hay armarios con paneles RJ-45 de diferentes fabricantes (Systimax en Plaza Mayor y alguno en Filosofía, Ortronics en Edificio C de EPS, etc.), por lo que en cada armario hay que instalar los paneles del mismo fabricante que está instalado en dicho armario.

Siempre que se pueda, el instalador utilizará las canaletas, bandejas y otras canalizaciones por donde se distribuyen todos los cables voz-datos del edificio. Esto sucederá, sobre todo, en las cercanías de los armarios de comunicaciones.

Allí donde no haya canalización, o sea, conforme los cables se vayan acercando al punto donde hay que instalar la caja de pared, el instalador debe instalar los cables utp con la canalización adecuada: tubos corrugados, canaletas pequeñas, etc.

En todos los sitios donde sea necesario hacer calos o agujeros en paredes para tender los cables, el instalador debe poner tapas registrables.

Las certificaciones de todos y cada uno de los cables instalados se entregarán a los servicios técnicos de la universidad, preferiblemente en fichero flw.

En la Facultad de Derecho y en los dos módulos de la facultad de Ciencias que se actualizaron en 2015 no es necesario instalar nuevo cableado.

Los latiguillos de parcheo en los armarios de comunicaciones, 110<->RJ-45 Cat6 y RJ-45<->RJ-45, Cat6A, serán suministrados por el adjudicatario.

Los latiguillos de servicio entre las rosetas y los APs, RJ-45<->RJ-45 Cat6A, de 50cms como mucho, serán suministrados e instalados por el adjudicatario.

Se han de suministrar mil quinientos sesenta y dos puntos de cableado como los descritos en este apartado.

- 1550 puntos para APs de interior.
- 12 puntos, para APs mesh de exterior, con los componentes y protecciones para exterior adecuadas. Tanto el cableado, como los 12 latiguillos RJ-45-RJ-45, 50cm, de estos casos, serán adecuados para intemperie.

4.10 Candados.

Los APs actualmente instalados en la universidad tienen un candado tipo Kensington para asegurarlos, con llave única compartida. Esos candados se van a reutilizar en este proyecto.

La universidad no puede tener una llave distinta para cada candado singular tipo Kensington. El ofertante puede seleccionar la marca y el modelo de candado tipo Kensington que considere más oportuno, siempre que todos los candados que suministre se abran con la misma llave. Además, el ofertante debe garantizar que la universidad podrá adquirir mas candados con esa misma llave en años posteriores.

Se han de suministrar e instalar mil trescientos cincuenta candados tipo Kensington.

4.11 Arandelas y tornillos de seguridad.

Los AP70 actualmente desplegados, disponen de una estructura de montaje metálica sobre la que puede asegurar el candado tipo Kensington. En 2005, el soporte metálico de los AP70 se aseguraba a la pared con un tornillo de seguridad.

Los APs actuales no suelen disponer de esa estructura metálica. Lo más habitual es que dispongan solamente de soportes plásticos poco resistentes.

Por tanto, es necesario proporcionar una arandela metálica que se fijará a la pared con tornillos de seguridad.

La referencia de los tornillos que se han de suministrar obligatoriamente, se puede encontrar en:

http://es.rs-online.com/web/p/tornillos-de-seguridad-a-prueba-de-manipulaciones/3007650/

La universidad dispone de destornillador adecuado y lo puede prestar durante la instalación.

La referencia para la arandela es el elemento 00678306 de la página 19 del catálogo de http://www.profesionaldesuministros.com/

Se han de suministrar e instalar mil quinientas cincuenta arandelas y seis mil doscientos tornillos de seguridad.

El resto de materiales y trabajos, tacos, agujeros, tornillos etc., y la maquinaria necesaria, taladros, escaleras, herramientas, etc., corren por cuenta del adjudicatario.

4.12 Cursos.

El adjudicatario debe impartir, en las instalaciones de la universidad, los cursos que se detallan en este apartado. Deben ser cursos enfocados a la instalación objeto de este pliego. Por tanto,

el profesorado puede ser personal técnico de la empresa ofertante, y no es necesario que sean impartidos por una empresa especializada en formación.

Curso	Duración.	Asistentes.
Curso de fundamentos y uso del *software* AAA ofertado.	Dos días.	Seis.
Curso de uso y configuración de los conmutadores de acceso.	Un día.	Seis.
Curso de uso y configuración de las controladoras inalámbricas.	Un día.	Seis.
Curso de uso y configuración de la herramienta de gestión.	Dos días.	Seis.
Curso de uso y configuración del portal de invitados.	Dos días.	Seis.

4.13 Documentación final.

La universidad requiere del adjudicatario la entrega de una documentación final de proyecto. No se trata de manuales o documentos genéricos del fabricante de los equipos, sino que deben ser documentos elaborados específicamente para esta instalación que incluirán:

- Interconexiones, relaciones y dependencias de todo el equipamiento instalado.
- Parámetros básicos globales: VLANES, direccionamiento IP, roles, políticas, etc., que se han configurado en todas las plataformas instaladas.
- Manuales de operación para las tareas más habituales que se suelen realizar en la nueva instalación.

4.14 Director de proyecto.

La empresa adjudicataria, durante toda la duración del contrato, designará un Director Técnico de Proyecto que tendrá los siguientes cometidos.

- Será el técnico que dispondrá de una visión más global de la red inalámbrica de la universidad. Conocerá las relaciones y dependencias establecidas entre todos los equipos objeto del mantenimiento.
- Tendrá conocimiento de todas las averías y funcionamientos anómalos que se detecten en los equipos objeto de este contrato. Esto tendrá especial importancia si están implicados varios tipos diferentes de equipos y/o protocolos. Debe proponer las medidas correctivas necesarias.
- Coordinará y supervisará las acciones que realicen los técnicos especialistas de cada uno de los equipos.
- Resolverá y evitará, informando previamente a los técnicos de la universidad, aquéllas acciones correctivas que pudieran llegar a ser incompatibles con los servicios prestados, o con otros equipos de la universidad, o que pudiesen mermar sustancialmente el rendimiento de cualquier sistema.
- Será el principal interlocutor sobre cuestiones técnicas de la empresa adjudicataria con la universidad. Esto no impide que en acciones puntuales, previamente conocidas y supervisadas por el Director del Proyecto, los especialistas de la empresa adjudicataria y los técnicos de la universidad acuerden sobre el terreno detalles menores, no esenciales, sobre las tareas a realizar.
- Supervisará, de forma coordinada con los técnicos de la universidad, las tareas que realice el Operador de Red.
- Las nuevas versiones de software de algunos componentes suponen un cambio drástico en su modo de funcionamiento y por tanto, ha de realizarse extremando el

cuidado. El Director de Proyecto ha de estar al tanto de lo que suponen las transiciones a nuevas versiones y planificarlas de la forma menos traumática posible. La empresa adjudicataria ha de arbitrar el apoyo y asistencia de todos los técnicos que sean necesarios.

- Mantendrá reuniones de seguimiento periódicas con los servicios técnicos de la universidad.
- Supervisará la entrega de la documentación final del proyecto.

El ofertante debe indicar el perfil del Director del Proyecto completo, y detallar la formación y la experiencia reciente que tenga en instalaciones similares.

4.15 Operador.

La empresa adjudicataria, durante toda la duración del contrato, desplazará a la Universidad, en el campus de Cantoblanco, de lunes a viernes y de 8:30 a 17:30 horas, con una hora para almorzar, un técnico cualificado, para la realización de trabajos diarios de operación de red:

- Colaboración e interlocución con los servicios técnicos de la universidad para llevar a cabo la nueva instalación objeto de este pliego.
- Supervisión y monitorización de la nueva red y de la existente, mediante las herramientas de gestión disponibles.
- Detección proactiva y primer nivel de diagnóstico de incidencias de red.
- Registro, tratamiento, notificación y escalado de incidencias de red de acuerdo con los procedimientos de operación establecidos.
- Interlocución con cuantos agentes sean necesarios para la resolución de incidencias (proveedores de servicios de comunicación y mantenimiento de equipos, usuarios afectados, otros departamentos de la UAM, etc.) de acuerdo con los mecanismos de interlocución establecidos.
- Gestión y control de la reparación o sustitución de elementos averiados.
- Control de trabajos programados en la red.
- Atención de incidencias notificadas por vía telefónica o telemática por los interlocutores autorizados de la universidad.
- Modificaciones básicas de configuración de equipos (altas, bajas o modificaciones de servicio, etc.) y coordinación con el resto de agentes implicados en las mismas (instalador de equipos, proveedor de enlaces, usuarios afectados, otros departamentos de la UAM, etc.) de acuerdo con los procedimientos de provisión de servicio establecidos.
- Obtención de estadísticas y elaboración de informes periódicos sobre la red, en la medida que las herramientas automáticas que tenga a su disposición lo permitan (no incluye el desarrollo de estas herramientas).
- Colaboración en el mantenimiento de la documentación de la red de la universidad.
- Colaboración con los servicios técnicos de la UAM en la atención a usuarios de la red inalámbrica, problemas, configuraciones, documentación, etc.
- Realización de todos los trabajos necesarios para habilitar nuevos servicios para congresos con asistentes externos a la UAM.
- Colaboración con otros técnicos de la empresa adjudicataria para la sustitución de APs averiados por otros de los que tenga disponibles la universidad.
- Supervisión y monitorización de los sistemas de RADIUS y *accounting*.

El técnico de la empresa adjudicataria colaborará con los operadores y técnicos de la universidad en los trabajos habituales de mantenimiento y gestión diaria de equipos activos para el buen desarrollo de las comunicaciones de la Universidad, y cooperará en el buen funcionamiento y coordinación de los trabajos a realizar, además de acompañar y dar acceso a

las instalaciones de comunicaciones a los técnicos de otras empresas externas, siguiendo siempre las indicaciones de la Universidad Autónoma de Madrid.

Se estima que el 99% de las tareas se realizarán en el campus de Cantoblanco y Medicina, y el 1% en el edificio de la Corrala, la residencia de La Cristalera y el Colegio Mayor Juan Luis Vives.

Los desplazamientos desde el campus de Cantoblanco a otros centros de la Universidad serán por cuenta del adjudicatario, debiendo éste facilitar medio de transporte propio a su técnico cuando se desplace.

Durante el mes de vacaciones estivales y durante los periodos de baja laboral superiores a tres días laborables del técnico, la empresa adjudicataria desplazará a la UAM otro técnico de igual o superior cualificación en sustitución.

Para la gestión de averías e incidencias, la Universidad Autónoma de Madrid cuenta con un servicio de "help-desk", en horario normal de trabajo, y un sistema informático disponible 24h. x 7 días.

La Universidad Autónoma de Madrid formará en el manejo del sistema informático de gestión de incidencias al técnico que el adjudicatario designe, y suministrará los medios adecuados para la utilización de dicho sistema en los locales de la Universidad.

El técnico asignado al contrato deberá tener el siguiente perfil:

- Técnico con formación profesional FPII.
- Experiencia demostrable en operación y mantenimiento de redes.
- CCNA.
- CCNA Security.
- CCNA Wireless.
- CCNP.
- CCNP Wireless.
- ACFE OmniAccess Wlan. (Alcatel)
- ACWA. (Aerohive)

5 Requerimientos a la empresa adjudicataria.

Dadas las características de la red, tamaño, complejidad, etc., y para garantizar el éxito del despliegue, el adjudicatario deberá presentar obligatoriamente copias de las siguientes certificaciones.

La universidad podrá requerir a los ofertantes cualquier original para resolución de dudas.

5.1 Certificaciones de Fabricante.

La tecnología propuesta debe tener una madurez e implantación en el mercado avaladas por un agente experto independiente, habiéndose elegido para ello el informe "Gartner Magic Quadrant - The Wired and Wireless LAN Access Infrastructure". Los productos propuestos para el arrendamiento deben pertenecer a alguno de los fabricantes situados en el cuadrante superior derecho de dicho informe Gartner del 2015, o el último publicado a la fecha del pliego.

El adjudicatario deberá disponer de las certificaciones del fabricante propuesto, que garanticen su conocimiento y capacidad técnica para realizar el diseño, despliegue y soporte posterior de la solución ofertada.

Las certificaciones requeridas lo serán según el fabricante de la solución presentada, es decir, el adjudicatario que presente una solución basada en un fabricante, deberá aportar las certificaciones de dicho fabricante y no las de otro.

Nivel de Partner.

- *Aruba Networks:*
  - Gold.
- *Cisco*
  - Gold Certified Partner y PSPP Education.

Personal Técnico red WLAN: Niveles de certificación en la solución inalámbrica propuesta con ingenieros certificados en dicha tecnología y fabricante, siendo consideradas válidas las certificaciones siguientes:

- *Aruba Networks:*
  - Mínimo 2 ACDX – Aruba Certified Design Expert.
  - Mínimo 2 ACMP – Aruba Certified Mobility Professional.
- *Cisco:*
  - Mínimo 2 CCNP Wireless – Cisco Certified Network Professional.

Personal Técnico AAA: Niveles de certificación de la solución de *Authentication, Autorization & Accounting* propuesta, con ingenieros certificados en dicha tecnología y fabricante, siendo consideradas válidas las certificaciones siguientes:

- *Aruba Networks:*
  - Mínimo 2 ACCP – Aruba Certified ClearPass Professional.
- *Cisco (Cumplir una de las dos siguientes):*
  - Mínimo 2 CCNP Seguridad – Cisco Certified Network Professional de Seguridad, o bien
  - Mínimo 2 SISA (Implementing Cisco Secure Access Solutions).

5.2 Otras Certificaciones Técnicas.

5.2.1 Ekahau.

Siguiendo la línea de garantizar un correcto despliegue y para minimizar los riesgos, será requisito indispensable que el adjudicatario disponga del certificado siguiente:

- **Ekahau**: Al menos, 1 ingeniero certificado Ekahau Certified Survey Engineer (ECSE).

5.2.2 Cableado.

Se han de presentar dos certificaciones.

- Una que demuestre la empresa instaladora del cableado ha sido homologada por el fabricante de los componentes de cableado.
- Otra en la que se demuestre que la empresa instaladora tiene alguna experiencia en el sistema de cableado 110, que está en el catálogo de cualquier fabricante, y del que la universidad tiene un gran parque instalado, pero es poco utilizado hoy en día.

Para el primer caso, basta con el certificado de homologación habitual, que debe estar vigente.

Para el segundo, basta con presentar el certificado en formación sobre sistemas 110 de algún empleado, o la certificación de alguna obra realizada por la empresa en sistemas 110. Por la antigüedad del sistema 110, no importa si estos certificados son viejos o han caducado.

5.3 Certificaciones de Calidad.

El ofertante debe disponer y presentar copia de las certificaciones siguientes:

- Gestión de la Calidad: ISO 9001:2008.
- Sistemas de Gestión Ambiental: ISO 14001:2004.
- Gestión de la Seguridad de la Información: ISO/IEC 27001:2013.

6 Forma de pago y opción de compra.

El abono del precio del contrato se efectuará en pagos mensuales fijos e iguales resultantes de dividir el importe de adjudicación entre los 48 meses de duración del contrato. El primer pago se realizará al mes de la fecha de inicio del contrato.

A la finalización del contrato, la UAM podrá ejercer la opción de compra sobre la totalidad de los equipos arrendados. El precio de adquisición será el que resulte de dividir el importe de adjudicación entre 48.

7 Mantenimiento.

Según se ha detallado en apartados anteriores, el licitante debe considerar la renovación de los APs, la instalación de cableado según determinen los estudios de cobertura, y la sustitución completa o ampliación de controladoras, licencias, etc. según sea necesario.

Además, a la vez que se realiza esta renovación, la red inalámbrica de la universidad, en todas sus fases, y en toda su complejidad durante la transición, debe ser soportada y mantenida en todos los aspectos y en todos sus componentes:

- Mantenimiento *hardware* de controladoras, *appliances*, fuentes, APs, *testers*, SFPs, etc.
- Mantenimiento completo de todo el *software* y las licencias: FreeRADIUS, BD de *accounting*, controladoras, Omnivista, Ekahau, etc.
- Los servicios técnicos de la universidad podrán enviar tantas consultas como sea necesario, y serán escaladas al fabricante siempre que se necesite.

Si hay algún periodo en el que haya infraestructura de dos fabricantes prestando servicio simultáneamente, ambas han de ser mantenidas completamente.

El adjudicatario debe hacerse cargo de la renovación anual, durante todo el periodo del contrato, de:

- La licencia Premium Pack del *software* Ekahau de la universidad.
- El soporte Gold, únicamente para el Air Check Wi-Fi Tester de Fluke 1.0 de la universidad.

7.1 Soporte y atención al cliente.

Los licitadores deberán incluir en su oferta técnica un servicio de soporte para la apertura, seguimiento, escalado y cierre de cualquier incidencia, por vía telemática, preferiblemente en formato portal web.

El canal telefónico deberá ser accesible, al menos, en horario laborable de 8:00 a 18:00 horas. El portal web será accesible 24 horas al día y 365 días al año.

Este servicio incorporará un sistema de información accesible por los responsables que designe la UAM y un protocolo de comunicación entre la UAM y el adjudicatario que, de común acuerdo, determine los procedimientos de apertura, seguimiento, escalado y cierre de incidencias. Se deberá indicar, entre otros, el grado de severidad de la incidencia.

Asimismo, a través del portal web, los responsables de la UAM podrán consultar información relevante acerca del servicio contratado, como por ejemplo:

- Inventario de servicios contratados.
- Estado de las incidencias en curso.
- SLAs del servicio.

7.2 Mantenimiento.

El mantenimiento será de aplicación tanto a los equipos físicos (incluyendo el microcódigo que pudiera ser necesario para su correcto funcionamiento, con independencia de que éste se almacene en cualquier tipo de memoria de sólo lectura), como a los equipos lógicos (sistemas operativos, programas y utilidades del sistema, compiladores, parches, etc.), que pudieran ser necesarios para corregir un funcionamiento anómalo de los equipos objeto de este pliego.

El mantenimiento es el área encargada de minimizar los tiempos de indisponibilidad de los equipos de la red, mediante la ejecución de acciones preventivas y correctivas sobre los elementos que forman parte del alcance del presente pliego.

Las ofertas deberán incluir una descripción de estas acciones considerando las siguientes definiciones:

- **Tipo de avería o Nivel de servicio**: Clasificación de las incidencias para la asignación del tiempo de respuesta asociado.

- **Tiempo de respuesta**: tiempo transcurrido entre la recepción del aviso por parte de la UAM y el inicio de las actividades por parte del adjudicatario, ya sea en modo remoto o en las dependencias del cliente final, según lo requiera la incidencia.

- **Tiempo de resolución**: tiempo transcurrido entre el inicio de las actividades por parte del adjudicatario y la resolución de la incidencia o la tarea solicitada.

La corrección y reparación de las averías pueden implicar la sustitución o reconfiguración de equipos, desplazamiento de personal, mano de obra, escaleras, herramientas, pequeño material (tornillos, tacos, canaleta, etc.), en cualquiera de las ubicaciones de la UAM, cuyos gastos correrán a cargo del adjudicatario.

7.2.1 Niveles de servicio

7.2.1.1 Nivel de servicio ampliado.

El mantenimiento de los equipos para los que se solicita un ***nivel de servicio ampliado*** se prestará asimismo en las dependencias de la UAM, previa petición telefónica o por correo electrónico, a cualquier hora del día o de la noche, de lunes a domingo, incluso festivos.

El sistema de monitorización 24x7x365 que se menciona más adelante, iniciará de motu propio las acciones necesarias para reparar los equipos a los que se les aplica este nivel de servicio para cumplir los SLAs, aunque la avería se produzca en horario no laboral.

Equipamiento de este pliego al que se aplica este nivel:

- Controladoras.
- *Software* AAA.
- Plataforma de gestión, siempre que se proporcione un *appliance* físico.

7.2.1.2 Nivel de servicio estándar.

El mantenimiento de los equipos para los que se solicita un ***nivel de servicio estándar***, se prestará en las dependencias de la UAM, previa petición telefónica o correo electrónico de lunes a viernes, entre las 9:00 y las 18:00.

Equipamiento de este pliego al que se aplica este nivel:

- APs.
- Conmutadores.

7.2.2 Tipos de incidencia

7.2.2.1 Incidencia grave.

Aquélla que impida el funcionamiento global de la red inalámbrica o el acceso de los usuarios a los servicios de la universidad:

- Pérdida completa de servicios de red por indisponibilidad de los controladores de red inalámbricos, el *software* AAA, la plataforma de gestión, o más del 50% de los APs.
- Degradación de gravedad alta del funcionamiento de la red inalámbrica, que contempla al menos los siguientes tipos de incidencias:
    - Reinicios críticos.
    - Malfuncionamiento de los controladores, el software AAA, la plataforma de gestión, o los APs que impidan la conexión de los usuarios a la red inalámbrica.
    - Problemas generales de tráfico en la red: imposibilidad de realizar cualquier tipo de conexión a través de la red inalámbrica.
    - Degradación de la capacidad de la red: el 50% o más de los equipos de usuario no pueden conectarse, el 50% o más de los APs están fuera de servicio, o el 50% de los servicios de red no son accesibles desde la red inalámbrica.

7.2.2.2 Incidencia media.

Aquélla que impida el funcionamiento de un requisito funcional importante en la red de datos:

- Cualquier avería que afecte a un número limitado de usuarios que no pueden conectarse a la red inalámbrica.
- Cualquier avería que afecte a un número limitado de APs o a alguna funcionalidad de la red inalámbrica.
- Cualquier avería que impida el acceso a algunos servicios de la universidad o que produzca carga injustificada en los controladores inalámbricos o en el software AAA.
- Degradación de gravedad media del funcionamiento de la red inalámbrica, que contempla al menos los siguientes tipos de incidencias:
  - Imposibilidad de realizar algún tipo de conexión a través de la red.
  - Intensidad de fallos superior a la normal en los equipos de este pliego.
  - Degradación de la capacidad de la red: más del 25% y menos del 50% de los equipos de usuario están fuera de servicio, más del 25% y menos del 50% de los enlaces están fuera de servicio, o más del 25% y menos del 50% de los servicios de red están fuera de servicio.
  - Reinicio largo o corto de equipos, no considerados críticos para el sistema.

7.2.2.3 Incidencia leve.

Todas las demás.

7.2.3 Tabla de SLAs.

El Tiempo Máximo de Respuesta (TMRP) y el Tiempo Máximo de Resolución (TMRS) de incidencias o solicitudes requeridos por la UAM son los siguientes:

Tipo de Incidencia o Solicitud	Horario ocurrencia	TMRP	TMRS
Servicio ampliado e Incidencia grave	Cualquiera	30 minutos	2 horas
Incidencia media	Laboral	2 horas	6 horas
	No laboral	4 horas	15 horas
Servicio estándar e Incidencia leve	Laboral	4 horas	1 día laborable
	No laboral	1 día laborable	2 días laborables

El licitador deberá indicar los Tiempos Máximos de Respuesta (TMRP) y Resolución (TMRS) de incidencias ofertados usando el siguiente formato:

Tipo de Incidencia o Solicitud	Horario ocurrencia	TMRP	TMRS
Servicio ampliado e Incidencia grave	Cualquiera		
Incidencia media	Laboral		
	No laboral		
Servicio estándar e Incidencia leve	Laboral		
	No laboral		

7.2.4 Repuestos.

La empresa garantizará, bajo su responsabilidad, la previsión y disponibilidad de cualquier clase de repuestos necesarios para el mantenimiento de los equipos amparados por el contrato. No obstante, si resultase imposible, o muy difícil su obtención, habrá de presentar un plan de contingencia en su plan de ejecución, para el caso de que no pudiera disponer de repuestos por causas ajenas a su control.

En caso de sustitución por avería de cualquier equipo, el equipo sustituido pasará a ser propiedad del adjudicatario, mientras que el equipo sustituto pasará a ser propiedad de la

Universidad, y se deberá incluir su número de serie en el contrato de mantenimiento que el adjudicatario tenga con el fabricante. El número de intervenciones y de repuestos no estará limitado.

Al efecto de diagnosticar y, en su caso, solucionar las incidencias que se presenten, el adjudicatario podrá establecer una conexión remota con los equipos a mantener siempre bajo los protocolos de control y seguridad establecidos por la UAM.

7.2.5 Mantenimiento preventivo.

El adjudicatario realizará, por cada equipo incluido en el contrato, al menos una revisión anual a lo largo del período de vigencia del contrato.

Estas revisiones se llevarán a cabo a solicitud de la UAM, y tendrán por objeto prevenir posibles averías y comprobar el óptimo funcionamiento del equipo o de cualquiera de sus componentes. Los trabajos a realizar durante las revisiones de carácter preventivo de los equipos físicos objeto del contrato dependerán de la naturaleza de los mismos. Genéricamente estos serán: la limpieza general externa e interna de los equipos, revisión de conectores, sustitución de elementos que estén averiados, ejecución de programas de diagnóstico de correcto funcionamiento, etc.

Para llevar a cabo estas tareas la compañía adjudicataria proveerá los equipos, los programas de diagnóstico y los medios de acceso adecuados al objeto de la revisión.

7.2.6 Programas

Suministro, instalación y configuración sin coste, a petición de la UAM, de las nuevas versiones de los programas, o *firmware*, asociados a los equipos del pliego, que las compañías fabricantes del mismo puedan sacar al mercado durante el período de vigencia del contrato, así como su documentación. La compañía adjudicataria deberá mantener informado a la UAM de la aparición de las nuevas versiones.

7.2.7 Servidor www de fabricantes.

Acceso privilegiado al servidor www de los fabricantes de los equipos, con el objeto de que el personal cualificado de la UAM pueda consultar la información técnica que necesiten para el uso y administración de los equipos.

7.2.8 Escalado.

La empresa adjudicataria realizará el escalado inmediato al Servicio Técnico del fabricante, de todas aquéllas incidencias que la empresa o la UAM consideren necesario sin coste adicional, de todos los equipos arrendados.

Se debe incluir documento en el que se haga constar la aceptación de este requisito.

7.3 Asesoramiento y consultoría.

La empresa adjudicataria asesorará a los servicios técnicos de la universidad en los proyectos de ampliación o mejora de los equipos.

7.4 Servicio de monitorización.

La empresa adjudicataria debe establecer un servicio de monitorización y recepción de alarmas de los equipos objeto de este pliego 24x7x365.

En coordinación con los técnicos de la universidad, el adjudicatario configurará los equipos objeto del contrato, para enviar alarmas al centro de monitorización de la empresa, respetando siempre los protocolos y medidas de seguridad en estos casos.

El centro de monitorización vigilará especialmente las caídas de equipos y las pérdidas globales de conectividad, aunque también recogerá y procesará mensajes sobre anomalías o fallos parciales del hardware: fallos en ventiladores, fuentes de alimentación, etc...

Dependiendo del nivel de servicio, ampliado o estándar, el centro de monitorización iniciará acciones correctivas inmediatas, incluso en fin de semana, o enviará aviso el Operador de Red y a la universidad para su resolución en la siguiente jornada laborable.

El adjudicatario proporcionará un acceso web a los técnicos de la universidad a la aplicación de monitorización con la que el adjudicatario está realizando el mantenimiento. Los técnicos de la universidad necesitan comprobar la disponibilidad de los equipos monitorizados por el adjudicatario. Este portal web tendrá un formato adecuado para acceder desde dispositivos móviles.

Las ofertas deberán incluir una descripción del Plan de Calidad y Disponibilidad de toda la red objeto del presente pliego que responda a los requisitos de calidad y disponibilidad detallados en los siguientes apartados.

8 Plan de Calidad del servicio.

8.1 Calidad de servicio

El licitador deberá indicar los parámetros de calidad de servicio que se compromete a cumplir.

Este conjunto de parámetros deberá estar basado en magnitudes suficientemente objetivas y acreditativas de la calidad del funcionamiento de la red de datos. Estos parámetros deberán ser medidos mensualmente y presentados a la UAM en un informe, en los cinco primeros días del mes siguiente.

8.2 Disponibilidad.

El adjudicatario deberá garantizar una disponibilidad de la red de datos objeto de este pliego superior al 99,9%. La disponibilidad se calculará en base a la siguiente fórmula:

Disponibilidad = 100 * ((Ttotal – Tind) / Ttotal)

Donde:

- Ttotal es el tiempo total en minutos del periodo medido, que para un mes son 43.200 minutos.
- Tind es la suma de los tiempos de indisponibilidad del sistema en minutos.

La Disponibilidad se calculará sobre una base mensual.

El adjudicatario deberá garantizar un tiempo mínimo entre fallos (TMEF) de la infraestructura inalámbrica arrendada de 8 días, salvo que dicho adjudicatario haya indicado un valor superior en su oferta.

8.3 Penalizaciones por incumplimiento de tiempos de respuesta y resolución.

Para garantizar el cumplimiento de los objetivos de calidad de servicio se establecen las siguientes penalizaciones, que se harán efectivas mensualmente.

Para los diferentes tipos de incidencia deberá tenerse en cuenta lo siguiente:

Tipo de Incidencia o Solicitud	Coste comprometido
Soporte ampliado e Incidencia grave	60% coste mensual del mantenimiento
Incidencia media	30% coste mensual del mantenimiento
Soporte estándar e Incidencia leve	5% coste mensual del mantenimiento

En el caso de no cumplirse los tiempos máximos de respuesta y de resolución de incidencias ofertados, el adjudicatario deberá compensar a la UAM de acuerdo con la siguiente tabla:

Porcentaje en que los tiempos empleados superan a TMRP y TMRS	Penalización a aplicar
Hasta un 50%	10% del coste comprometido
Entre un 50% y un 100%	20% del coste comprometido
Entre un 100% y un 150%	30% del coste comprometido
Entre un 150% y un 200%	40% del coste comprometido
Superior a 200%	50% del coste comprometido

Dicho porcentaje se calculará como sigue:

Porcentaje desviación = ((TRX / TMRX) - 1) * 100

Donde:

- TRX puede ser el Tiempo de Respuesta (TRP) ó el Tiempo de Resolución (TRS) de la incidencia expresado en horas.
- TMRX puede ser el Tiempo Máximo de Respuesta (TMRP) ó el Tiempo Máximo de Resolución, (TMRS), expresado en horas.

8.4 Penalizaciones por incumplimiento del Tiempo mínimo entre Fallos.

En el caso de incumplimiento del Tiempo mínimo entre Fallos, TMEF, el adjudicatario deberá compensar a la UAM de acuerdo con el siguiente criterio.

Para el cálculo de la penalización por una frecuencia de fallos superior a la máxima exigible se aplicará la siguiente fórmula (válida cuando TMEF es mayor que N):

$R = (1 - (N / TMEF)) \times Cdia$

Donde:

- R: Penalización o compensación económica.
- TMEF: Tiempo mínimo entre fallos.
- N: Número de días discurridos desde el último fallo en el sistema.
- Cdía: Coste del contrato referido a un día. Se calcula como el Coste fijo mensual dividido por 30.

8.5 Penalizaciones por incumplimiento de disponibilidad.

Por otra parte, en el caso de incumplimiento de la disponibilidad ofertada, el adjudicatario deberá compensar a la UAM de acuerdo con la siguiente tabla:

Porcentaje de desviación de disponibilidad	Penalización (% facturación mensual)
No hay desviación (disponibilidad superior al 99,9%)	0%
Disponibilidad entre 99,9% y 99,85%	3%
Por cada 0,05% adicional	3% adicional

8.6 Cálculo total de penalizaciones.

La penalización mensual total se calculará como la suma de las penalizaciones debidas a los diferentes criterios considerados por el adjudicatario.

Dicha penalización mensual total no podrá superar el 50% de la facturación mensual.

No se contabilizarán a efectos de penalización las horas que el sistema permanezca parado por causas ajenas al adjudicatario, tales como fallo generalizado en el suministro eléctrico, o mala operación de los mismos por el personal de la UAM.

Tampoco se contabilizarán a efectos de penalización las horas que el sistema permanezca parado por causas de fuerza mayor, tanto naturales (terremotos, inundaciones, etc.), como artificiales (sabotajes, atentados, etc.).

No obstante, en estos casos, el adjudicatario considerará el sistema de la UAM como de alta prioridad para la puesta en marcha de los servicios prestados.

9 Documentación a entregar en la oferta técnica.

A continuación se muestra un listado de chequeo para todos los datos técnicos que se han de entregar en las ofertas.

En el sobre C hay que entregar el número y la descripción de todos los elementos técnicos ofertados, y todos los documentos necesarios para comprobar que se cumplen las especificaciones mínimas descritas en este pliego.

En el sobre D hay que incluir los documentos necesarios para poder asignar correctamente los puntos por mejoras que figuran en el pliego de cláusulas administrativas.

Si no se cumple CUALQUIERA de las características mínimas descritas en este documento, la oferta técnica será rechazada.

Cualquier característica de los equipos debe ser demostrada con la hoja de datos de producto u otros documentos del fabricante.

Cualquier otra característica adicional, no citada en este documento, que el ofertante considere interesante para la universidad, debe ser justificada, también, con documentos del fabricante.

9.1 Estudios de cobertura.

- Confirmación de la utilización del software Ekahau para realizar los estudios de cobertura de interior.
- Materiales y componentes, número de APs, pértigas, baterías, etc., que se utilizarán para el estudio inicial.
- Experiencia y formación de los técnicos que realizarán los estudios de cobertura.

9.2 Controladoras.

- Modelo y cantidad de controladoras que se suministrarán. Obligatorio conseguir redundancia N+1.
- Hoja de datos, y otros documentos del fabricante, con TODAS las características mínimas señaladas.
- Hoja de datos, y otros documentos del fabricante, que permitan la asignación de los puntos de mejoras. Sobre D.
- Número y tipos de licencias suministradas.

9.3 APs de interior.

- Modelo y cantidad de APs de interior que se suministrarán.
- Hoja de datos, y otros documentos del fabricante, con TODAS las características mínimas señaladas.
- Hoja de datos, y otros documentos del fabricante, que permitan la asignación de los puntos de mejoras. Sobre D.

9.4 APs de exterior.

- Proyecto propuesto por el ofertante para los estudios de cobertura e instalación de los APs.
- Modelo y cantidad de APs de exterior que se suministrarán. Si se suministran antenas externas, numero, modelo y hoja de datos.
- Modelo y cantidad de soportes (farola, pared, voladizo, etc.) a suministrar.
- Hoja de datos, y otros documentos del fabricante, con TODAS las características mínimas señaladas.
- Hoja de datos, y otros documentos del fabricante, que permitan la asignación de los puntos de mejoras. Sobre D.

9.5 Candados, arandelas y tornillos de seguridad.

- Listado a suministrar. Modelo y cantidad.

9.6 Herramienta de gestión.

- *Hardware* y *software* suministrado. Número y tipo de licencias si fuese el caso.
- Listado de las funcionalidades mínimas solicitadas para este apartado, que se cumplen, con documento del fabricante donde se señala cada una de las características que se mencionan. Se subraya de nuevo la especial importancia de la funcionalidad multifabricante de la herramienta ofertada.
- Hoja de datos, y otros documentos del fabricante, que permitan la asignación de los puntos de mejoras. Sobre D.

9.7 *Software* AAA.

- *Hardware* y *software* suministrado.
- Hoja de datos, y otros documentos del fabricante, con TODAS las características mínimas señaladas.
- Hoja de datos, y otros documentos del fabricante, que permitan la asignación de los puntos de mejoras. Sobre D.
- Descripción del montaje que se realizará para conseguir el objetivo solicitado sobre el *accounting*.

9.8 Conmutadores de acceso.

- Modelo y cantidad de conmutadores que se suministrarán.
- Hoja de datos, y otros documentos del fabricante, con TODAS las características mínimas señaladas.
- Hoja de datos, y otros documentos del fabricante, que permitan la asignación de los puntos de mejoras. Sobre D.
- Enumeración de los SFPs y todos los latiguillos que se suministrarán e instalarán.
- Tabla del Anexo III de este documento, editada para incluir el número y modelo de conmutadores a instalar en cada armario de comunicaciones.

9.9 Cableado.

- Cantidades, marcas y componentes de cableado que se utilizarán.

9.10 Cursos.

- Guion y duración de los cursos solicitados en este pliego.

9.11 Operador de red y Director de proyecto.

- Formación y experiencia del operador de red propuesto por el ofertante.
- Formación y experiencia del director de proyecto propuesto por el ofertante.

9.12 Mantenimiento.

- Descripción del servicio de soporte ofertado para apertura, seguimiento, escalado y cierre de incidencias.
- Confirmación del equipamiento adscrito a cada nivel de servicio, ampliado o estándar, y de los tipos de incidencias descritos en este pliego.
- Entrega de la Tabla de SLAs que propone el ofertante.
- Enumeración de los equipos de repuesto de los que dispone el ofertante para sustitución rápida del equipamiento descrito en este pliego.
- Plan de contingencia para el caso de no disponer de repuestos.
- Sistema de conexión propuesto por el ofertante para acceso y configuración remota.
- Confirmación de que, durante el periodo del contrato, no hay limitación en:
    - El número de intervenciones y de repuestos necesarios para realizar reparaciones.
    - El número de incidencias que se podrán escalar al fabricante.
    - El suministro de versiones de programas o *firmware* del equipamiento ofertado, su instalación y configuración.
- Confirmación del acceso privilegiado, para los servicios técnicos de la universidad, al servidor www del fabricante.
- Descripción del servicio de monitorización y alarmas 24x7x365, y los procedimientos a seguir en caso de avería.

9.13 Plan de Calidad.

- Aceptación de las penalizaciones descritas en este apartado del pliego.

9.14 Documentación de proyecto.

Los licitadores deben entregar un proyecto completo de suministro e instalación de componentes y trabajos, que incluya:

- Resumen ejecutivo:
  - Deberá indicar que la solución cumple con los requerimientos mínimos
  - Descripción de la solución y de los componentes propuestos
- Diseño de la solución y funcionalidades de los componentes en base a la estructura indicada en el capítulo *¡Error! No se encuentra el origen de la referencia..-¡Error! No se encuentra el origen de la referencia.*
- Descripción de los servicios profesionales incluidos. Esta descripción deberá incluir el planteamiento de ejecución del proyecto y metodologías del licitador.
- La universidad quiere hacer hincapié en la necesidad de que se detallen y se confirmen algunas tareas y trabajos, a las que el ofertante deben comprometerse obligatoriamente.
  - Estudios de cobertura.
  - Instalación y configuración de todo el equipamiento objeto de este pliego.
  - Ajuste y adaptación de la nueva infraestructura y del todo el *software* instalado, para que se integre completamente con el equipamiento ya existente.
  - Entrega de documentación sobre procedimientos y usos de la nueva infraestructura, y sobre los procedimientos y usos que afectan a la infraestructura que no sea sustituida en este proyecto.
- Planificación estimada del proyecto. Deberá incluirse, también, la planificación en formato Microsoft Project. Se deberá incluir, al menos:
  - Estimaciones de entrega del equipamiento.
  - Fases y tareas del despliegue.
  - Interdependencia: tareas llave para realizar otras tareas.
  - Materiales o componentes de cada fase.
  - Personas implicadas en cada tarea.

Es obligatorio entregar archivo Project de toda la instalación en la oferta.

10 Seguridad y confidencialidad de la información.

10.1 Seguridad y confidencialidad de la información.

El adjudicatario queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato (especialmente los de carácter personal), que no podrá copiar o utilizar con fin distinto al que figura en este pliego, ni tampoco ceder a otros ni siquiera a efectos de conservación.

El adjudicatario quedará obligado al cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Especialmente en lo indicado en el artículo 12 de la Ley Orgánica 15/1999, que a continuación se transcribe:

"Artículo 12.- Acceso a datos por cuenta de terceros La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna

otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento de la información únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas."

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el Artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier otro soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

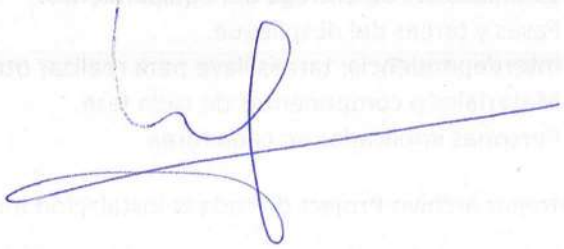
En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que se hubiera incurrido personalmente".

10.2 Propiedad intelectual de los trabajos realizados

El contratista acepta expresamente que los programas desarrollados, en su caso tanto fuentes como ejecutables, y de los derechos de explotación de las aplicaciones informáticas al amparo del presente contrato corresponden únicamente a la Universidad Autónoma de Madrid, con exclusividad y a todos los efectos.

Madrid, 30 de septiembre de 2016.

La Directora de Tecnologías de la Información,



Fdo.: María José García Rodríguez.

Esta Gerencia, por delegación del Sr. Rector de esta Universidad, de fecha 10-04-2015 (BOCM de 17-04-2015) ha resuelto aprobar el presente Pliego de Prescripciones Técnicas.

Madrid, 05-10-2016
EL GERENTE,

Teodoro Conde Minaya

11 Anexo I. Sistema de virtualización.

El sistema de virtualización de la Universidad Autónoma de Madrid está basado en software vCenter Server 6.0 y ESXi 6.0.

Para el despliegue de máquinas en la plataforma, lo óptimo, siempre que sea posible, es desplegar la OVA del fabricante del aplicativo, pues dicha OVA estará optimizada y certificada por el fabricante. Si esto no fuera posible, la UAM tiene como preferencia el despliegue dentro de su plataforma virtual, máquinas con sistema operativo RHEL 7.

Como excepción, y con una justificación adecuada, se podrían desplegar maquinas con sistema operativo Windows 2012 Server.

12 Anexo II. Tipos de APs y paneles en los armarios actuales.

A continuación, y por cada armario de comunicaciones de la universidad, figuran los APs instalados actualmente, y los tipos de paneles de cableado.

Edificio	AP					Tipo de
Armario	70	105	205	225	175	Panel
Biológicas						
042	6					110
043	6					110
055	7					110
056	11					RJ-45
Psicología						
044	9					110
045	11					110
046	2					110
075	5					110
Bib. Ciencias / Pabellón C						
070	6			1		110
071	2					110
072	1					110
073	8					110
Filosofía y Profesorado						
007	6				1	110
008	7					110
009	7					110
010	4					110
011	10					110
012	6					110
013	11					110
014	7					RJ-45
015	4					110
Económicas						
016	11					110
017	10					RJ-45
018	5					110
019	8					110

Edificio	AP					Tipo de
Armario	70	105	205	225	175	Panel
020	7					110
021	11					110
022	7					110
024	7					RJ-45
Ciencias						
026	3	3				110
027	6					110
054	7					110
028	14					110
029	10					110
030	7	1				110
031	6					110
032	4					110
033	7		17			110
034	7		16			110
035	10			1		110
037	12	1				110
047	2					RJ-45
Rectorado						
025	18	1			1	110
Pabellón A						
001	2					110
Bib. Humanidades						
002	8					110
Polideportivo						
004	1	2				110
Pabellón Norte						
005	2					110
Pabellón D						
006	2					110
Piscina						
050	2					110
Segainvex						
038	2					110
Esc. Infantil						
057		1				110
Tec. Alimentos						
058	3					110
Altas Energías						
060	1					110
APADUAM						
076	1					110
CMAM						

Edificio Armario	AP					Tipo de Panel
	70	105	205	225	175	
059	3					110
Cristalera						
701	3					RJ-45
702	6					RJ-45
Oficina Acogida						
083		1				RJ-45
EPS						
048	6			1		RJ-45
049	5					RJ-45
051	3					RJ-45
052	5					RJ-45
062				2		110
064	2	1				110
078	5					RJ-45
079	4					RJ-45
080	5					RJ-45
081	4					RJ-45
082	4					RJ-45
Plaza Mayor						
091		3				RJ-45
092		3		1	1	RJ-45
093		3				RJ-45
094		2				RJ-45
095		2				RJ-45
096		2			1	RJ-45
097		4				RJ-45
099		3		1		RJ-45
Medicina						
501	4					110
502	6	1				110
503	5					110
504	1	2				110
505	4			1		110
506	2					110
507	2					110
508	1	2				RJ-45
509	1					RJ-45
Corrala						
705	2	1				110
706	6					110
Colegio Mayor						
601	5		30			110
Derecho						
039			10			110
040			12			110
041		3	42	2		110
074		1	17	1		110
TOTAL	431	43	144	11	4	

13 Anexo III. APs a instalar. Puertos PoE y conmutadores a suministrar.

Basada en la experiencia de la universidad con el proyecto piloto, en la siguiente tabla aparecen las previsiones de APs Básicos que hay que instalar en cada armario.

Y se indica el número de puertos PoE que hay que suministrar, **como mínimo**, en cada armario de comunicaciones. No se admitirá que los conmutadores suministrados proporcionen alimentación en una cantidad menor que la detallada en esta tabla.

Como ya se ha explicado en el apartado correspondiente, en cada armario de comunicaciones, los conmutadores suministrados deben dar potencia suficiente para los APs Básicos previstos y un cierto margen para algún AP PoE y/o PoE+ adicional.

Para facilitar la entrega de documentación y la revisión, por los servicios técnicos de la universidad, de las ofertas presentadas, se han añadido dos columnas vacías, para que los ofertantes detallen los tipos de conmutadores, y las cantidades de los mismos, que proponen instalar en cada armario de comunicaciones.

Edificio Armario	Tipo de Panel	Previsiones de APs Básicos nuevos a instalar.	Puertos PoE mínimos a instalar.	Conmutador tipo A.	Conmutador tipo B.
Biológicas					
042	110	18	21		
043	110	18	21		
055	110	21	24		
056	RJ-45	33	36		
Psicología					
044	110	27	30		
045	110	33	36		
046	110	6	9		
075	110	15	18		
Bib. Ciencias / Pabellón C					
070	110	21	24		
071	110	6	9		
072	110	3	6		
073	110	24	27		
Filosofía y Profesorado					
007	110	21	24		
008	110	21	24		
009	110	21	24		
010	110	12	15		
011	110	30	33		
012	110	18	21		
013	110	33	36		
014	RJ-45	21	24		
015	110	12	15		
Económicas					
016	110	33	36		
017	RJ-45	30	33		

Edificio Armario	Tipo de Panel	Previsiones de APs Básicos nuevos a instalar.	Puertos PoE mínimos a instalar.	Conmutador tipo A.	Conmutador tipo B.
018	110	15	18		
019	110	24	27		
020	110	21	24		
021	110	33	36		
022	110	21	24		
024	RJ-45	21	24		
Ciencias					
026	110	18	21		
027	110	18	21		
054	110	21	21		
028	110	42	45		
029	110	30	32		
030	110	24	27		
031	110	18	21		
032	110	12	15		
033	110	21	41		
034	110	21	40		
035	110	33	36		
037	110	39	42		
047	RJ-45	6	9		
Rectorado					
025	110	57	60		
Pabellón A					
001	110	6	6		
Bib. Humanidades					
002	110	24	27		
Polideportivo					
004	110	9	12		
Pabellón Norte					
005	110	6	9		
Pabellón D					
006	110	6	9		
Piscina					
050	110	6	9		
Segainvex					
038	110	6	9		
Esc. Infantil					
057	110	3	6		
Tec. Alimentos					
058	110	9	12		
Altas Energías					
060	110	3	6		

Edificio Armario	Tipo de Panel	Previsiones de APs Básicos nuevos a instalar.	Puertos PoE mínimos a instalar.	Conmutador tipo A.	Conmutador tipo B.
APADUAM					
076	110	1	4		
CMAM					
059	110	9	12		
Cristalera					
701	RJ-45	9	12		
702	RJ-45	18	21		
Oficina Acogida					
083	RJ-45	1	4		
EPS					
048	RJ-45	21	24		
049	RJ-45	15	18		
051	RJ-45	9	12		
052	RJ-45	15	18		
062	110	6	9		
064	110	9	12		
078	RJ-45	15	18		
079	RJ-45	12	15		
080	RJ-45	15	18		
081	RJ-45	12	15		
082	RJ-45	12	15		
Plaza Mayor					
091	RJ-45	9	12		
092	RJ-45	12	15		
093	RJ-45	9	12		
094	RJ-45	6	9		
095	RJ-45	6	9		
096	RJ-45	6	9		
097	RJ-45	12	15		
099	RJ-45	12	15		
Medicina					
501	110	12	15		
502	110	21	24		
503	110	15	18		
504	110	9	12		
505	110	15	18		
506	110	6	9		
507	110	6	9		
508	RJ-45	9	12		
509	RJ-45	1	4		
Corrala					
705	110	9	12		
706	110	18	21		
Colegio Mayor					
601	110	20	53		

Edificio Armario	Tipo de Panel	Previsiones de APs Básicos nuevos a instalar.	Puertos PoE mínimos a instalar.	Conmutador tipo A.	Conmutador tipo B.
Derecho					
039	110	0	11		
040	110	0	13		
041	110	0	48		
074	110	0	20		
TOTAL		1442			

Como se ha indicado en el apartado "4.4.3 Cantidades de Puntos de Acceso", a este cálculo de APs Básicos a instalar, hay que sumar los 58 APs para el edificio Trimodular que será incorporado a la red de la universidad durante la ejecución del proyecto descrito en este documento.

Además, hay que suministrar 50 APs de Altas Prestaciones y 27 de APs de Exterior. 12 de los APs de Exterior irán con cableado de datos/alimentación, y los 15 restantes sin cableado de datos, pero con alimentación adicional que ha de instalar el adjudicatario.

Para el edificio Trimodular no hay que suministrar conmutadores. Por eso no aparecen los armarios de ese edificio en esta tabla.

14 Anexo IV. Tabla de mejoras de la oferta.

Con el fin de facilitar a los servicios técnicos de la universidad la revisión y comprobación de las mejoras sobre el pliego que presenta cada oferta, se adjunta una tabla tipo que debe presentar debidamente cumplimentada cada ofertante en el sobre D.

Los ofertantes deben adjuntar en este apartado los documentos del fabricante que dan fe de que las mejoras son reales.

Mejora sobre el pliego.	**Si o No.**	**Cantidad.**
Puntuación adicional por las controladoras.		
Redundancia 1+1, en vez de N+1, y configuración de forma que en caso de caída no hay impacto en los usuarios y en las aplicaciones.		
Las controladoras pueden cambiar los ventiladores en caliente.		
Treinta mil dispositivos simultáneos por cada controladora suministrada.		
Las controladoras disponen de *statefull firewall.*		
Capacidad de personalizar los derechos de acceso a partir de la respuesta del servidor DHCP, para permitir a PCs y MACs acabar los scripts de red y arranques de red.		
Establecimiento de túneles seguros vía IPSEC/GRE a un equipo genérico de red, localizado en la DMZ, para facilitar el despliegue y reducir costes.		
La controladora dispone de servicio VPN. Acepta clientes inalámbricos sin *software* 802.1X que usen *software* VPN.		
Capacidad para establecer tiempo de uso basado en el valor de ancho de banda establecido para limitar la velocidad y bloquear puertos por SSID.		
Puntuación adicional por los APs Básicos.		

APs 4x4:3SS.		
Las radios de los APs hacen Análisis de Espectro para detectar Interferencias no Wi-Fi y servir clientes de forma simultánea.		
Las radios de los APs hacen Análisis de Espectro con una resolución de 5MHz.		
Dos interfaces Ethernet y posibilidad de configurar LACP con ambos.		
Soporte de 5Gbs en uno de los dos interfaces Ethernet.		
Los APs se suministran con *Bluetooth Low Energy* (BLE) incorporado.		
Los APs funcionan con todas las prestaciones 802.11ac con consumo PoE en vez de PoE+.		
Suministro de APs Básicos adicionales, para ampliaciones y sustitución rápida.		
Puntuación adicional por los APs Altas Prestaciones.		
APs con radio de 5GHz 4x4:4SS.		
Soporte de 5Gbs en uno de los dos interfaces Ethernet.		
Soporte de doble radio de 5GHz.		
Los APs se suministran con *Bluetooth Low Energy* (BLE) incorporado.		
Suministro de APs de Altas prestaciones adicionales, para ampliaciones y sustitución rápida.		
Puntuación adicional por los APs de exterior.		
APs 802.11ac Wave 2.		
Posibilidad de configuración en Daisy Chain.		
Suministro de un AP de Exterior adicional, para ampliaciones y sustitución rápida.		
Puntuación adicional por los conmutadores.		
Equipos stackables.		
Soporte de transceivers de terceros.		
AP Rogue Isolation.		
Soporte básico de OSPF. Que permita al menos definir la pertenencia los interfaces a un área OSPF.		
El conmutador permite configurar puertos para establecer un túnel contra el controlador de movilidad. El puerto funciona como un puerto más del controlador, aislado de la red local presente en el conmutador.		
Garantía del fabricante de reemplazo de los conmutadores (RMA), actualizaciones de software y parches para vulnerabilidades, después del EoS, sin pago adicional. En años.		
Suministro de puertos de conmutador adicionales con respecto a lo solicitado en el Anexo III del PPT.		
Puntuación adicional por la herramienta de Gestión.		
La plataforma incluye módulo de procesamiento de datos Netflow y/o S-flow.		
La plataforma incluye un módulo de monitorización de aplicaciones.		
La plataforma incluye módulo de monitorización específico del entorno SDN.		
Puntuación adicional por el *software* AAA, *accounting*, portal de invitados y provisión automática de dispositivos.		
Capacidad para trescientas autenticaciones por segundo.		
Capacidad para que se utilicen los mismos perfiles de usuario en toda la infraestructura suministrada: la red inalámbrica y los conmutadores de acceso.		
Compatibilidad con los estándares definidos por TNC (*Trusted Network*		

Connect) con especial foco en el estándar 802.1X.	
El sistema dispone de plantillas precargadas para una puesta en marcha rápida y sencilla del servicio de Eduroam.	