UNIVERSIDAD DE BURGOS | Servicio de Informática y Comunicaciones

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO, CONFIGURACIÓN Y MANTENIMIENTO DE PUNTOS DE ACCESO WI-FI

Contenido

1. OBJETO

El objeto de este pliego es la contratación por la Universidad de Burgos (en adelante, UBU) del suministro de **183 puntos de acceso WI-FI (AP)** y la migración de todo el sistema (557 puntos de acceso) a una arquitectura de gestión centralizada en la nube que permita administrar de forma unificada toda la infraestructura, tanto cableada como WI-FI, incluyendo las correspondientes licencias, así como los servicios de configuración, soporte y garantía durante un período de **3 años**.

2. SITUACIÓN ACTUAL

En la Universidad de Burgos, contamos actualmente con:

- Un total de 537 puntos de acceso WI-FI (AP) HP Aruba

- De los cuales 163 son de las series 2xx y 3xx
- Licencias Aruba Mobility Máster: 538
- Licencias HPE Aruba Networking Management Software (AirWave): 530
- Plataforma de gestión unificada en la nube (Aruba Central) para la administración de la red cableada

La Universidad desea reemplazar los puntos de acceso de la red inalámbrica de la serie 200 que actualmente están en fin de vida útil (end-of-life) por otros de la serie 6xx.

Adicionalmente, se desea disponer de una plataforma en la nube que permita gestionar todos los dispositivos de red (switches, routers, puntos de acceso Wi-Fi) desde un único panel, evitando el uso de diversas herramientas y reduciendo la complejidad operativa. Este tipo de plataformas en la nube permiten aplicar políticas de seguridad homogéneas en los dispositivos, reforzando la protección frente a ciberamenazas.

3. ALCANCE

En este el contrato se incluyen las siguientes necesidades:

a. Suministro:

- Suministro de 183 WI-FI (AP) HP Aruba del modelo 635 o equivalente.
- Elementos de sujeción (kits de montaje) para los 183 AP suministrados
- Licencias correspondientes a 557 AP totales para su conexión a una solución de gestión centralizada en la nube, compatible con todo el equipamiento de red actual de la UBU y el suministrado, que permita administrar de forma unificada toda la infraestructura, tanto cableada como WI-FI.
- Suministro de un equipo portátil o tablet para comprobar el funcionamiento de WI-FI 6E.

b. **Servicios:**

Configuración de 163 AP de las series 2xx y 3xx por los del nuevo modelo suministrado. Integración de todos los AP (557) en la solución de gestión centralizada en la nube. No se incluye la instalación física ni el cableado que será por cuenta de la universidad.

Formación: se incluirán dos jornadas formativas (**10h**) sobre Aruba Central.

c. **Mantenimiento:** el equipamiento a mantener será:

- Los APs suministrados.
- Todas las licencias suministradas para la integración de los dispositivos en la solución de gestión centralizada en la nube.

4. REQUISITOS

a) El equipamiento de los puntos de acceso suministrados debe integrarse con el resto de la arquitectura de red existente en la Universidad de Burgos, y con el sistema gestor de la red de comunicaciones **(ver ANEXO 1).**

b) La solución posibilitará disponer de una **arquitectura de gestión centralizada en la nube** que permita administrar de forma unificada toda la infraestructura de red, tanto cableada como WI-FI **(ver ANEXO 2).** Se proporcionarán, tanto el equipamiento hardware, como los servicios necesarios para su puesta en producción, integrando **la totalidad de puntos de acceso (AP)** en la solución centralizada en la nube, siendo esta la única plataforma gestora tanto para la red WI-FI como para la red cableada.

c) Se requiere poner a disposición del contrato al menos dos ingenieros certificados en las tecnologías objeto del contrato (certificados emitidos por el fabricante) y con experiencia de, al menos, 2 años en proyectos similares.

d) Se requiere que la empresa presente certificación que le acredite como Partner emitida por el fabricante de los equipos suministrados.

5. PLAZO DE ENTREGA

El plazo máximo para la entrega y configuración del suministro será **3 meses** a contar desde el día siguiente a la firma del contrato.

6. GARANTÍA

Se aplicarán las garantías comerciales y servicios postventa según lo establecido en el Real Decreto-ley 7/2021, de 27 de abril. La garantía de los equipos será de al menos **tres años** a contar desde la fecha de entrega de estos.

La Universidad requiere que todos los equipos suministrados estén respaldados mediante contratos de soporte en vigor del fabricante de los equipos, durante todo el periodo de cobertura del servicio.

Se deberá garantizar la existencia de soporte completo del fabricante y de repuestos durante al menos 6 años desde la firma del contrato.

7. SOPORTE Y MANTENIMIENTO

La empresa adjudicataria proporcionará soporte on-line y telefónico para la resolución de averías o malfuncionamiento del equipamiento suministrado. **El horario de soporte on-line será 7 días a la semana durante las 24 horas del día**. El horario laboral será como mínimo de **7h de lunes a viernes incluyendo obligatoriamente la franja de 9 a 14h (Hora Central europea - CET)**.

El soporte incluirá los desplazamientos y la intervención hardware en el lugar de instalación de los equipos, así como la entrega y recogida de las piezas.

Si se produjese una avería de hardware en los elementos suministrados, se suministrarán e instalarán por parte de la empresa adjudicataria los elementos necesarios para su reparación. En el caso de que se haga necesaria la retirada del equipo averiado, se proporcionará para su sustitución un equipo del mismo modelo y fabricante, en el tiempo especificado según las prioridades anteriores. En caso de no ser posible la sustitución por el mismo modelo, se realizará la sustitución por un punto de acceso compatible con mejores características previa aprobación por el Área de comunicaciones del Servicio de Informática y Comunicaciones. Estos elementos pasarán a ser propiedad de la universidad, al tiempo que los sustituidos pasarán a propiedad del adjudicatario.

Cuando se proceda a la sustitución de cualquier equipo, la empresa adjudicataria realizará una reinstalación del software y de los ficheros de configuración propios del equipo original, de forma que el nuevo equipo pueda prestar todas las funcionalidades

que se encontraban operativas en el equipo averiado antes del fallo (salvo que se acuerde lo contrario si las circunstancias lo desaconsejasen).

Los tiempos máximos de sustitución del hardware serán 8h, a partir de la comunicación de la incidencia.

La empresa adjudicataria deberá garantizar, la previsión y disponibilidad de cualquier clase de repuesto necesario para el mantenimiento de los equipos, explicitando documentalmente en su oferta la existencia de repuestos de dichos equipos. El transporte y la reposición de piezas, se realizará sin coste adicional para la UBU.

En el caso de producirse el fallo de un equipo por un error de su software interno, deberá proveerse a la Universidad de Burgos de la actualización correspondiente sin cargo alguno. La versión de software que se suministre deberá ser compatible con las funcionalidades operativas en el equipo averiado antes del fallo. La empresa adjudicataria será responsable de la configuración del mismo con la nueva versión sin coste adicional para la Universidad.

Se incluirá sin coste en el alcance del contrato la instalación de todas las actualizaciones que la UBU considere adecuadas, durante la vigencia del contrato.

8. RESPONSABILIDADES EN DECISIONES TÉCNICAS

El personal del Área de Comunicaciones del Servicio de Informática y Comunicaciones (SIC), es responsable del óptimo funcionamiento de las infraestructuras objeto del contrato. Por ello, cualquier decisión que afecte a la conexión, parada, modificación de configuraciones, sustitución, etc. del equipamiento objeto del contrato, debe ser consensuada previamente con los miembros de dicho Área.

Las actualizaciones deberán estar justificadas mediante la emisión de un informe en el que el adjudicatario detalle las causas que motivan la actualización. Una actualización no ocasionará perjuicio sobre el servicio prestado ni sobre los niveles de calidad del mismo.

En caso de que fuera necesario interrumpir la prestación de algún servicio o funcionalidad, se acordará con los responsables del SIC la fecha y hora de realización de la parada de manera que la incidencia por el corte del servicio sea la mínima posible.
Llegado el caso de que una solución adoptada sin consentimiento del personal del Área de Comunicaciones del Servicio de Informática y Comunicaciones provoque posteriormente mal funcionamiento o interrupciones del servicio, se podrá proceder a una sanción económica proporcional al número de horas de fallo provocadas por dicha anomalía.

9. SEGURIDAD DE LA INFORMACIÓN

La configuración de las infraestructuras deberá cumplir las medidas especificadas por el Esquema Nacional de Seguridad para un sistema de **categoría media**.

Las configuraciones deberán ajustarse a lo establecido en la Guía CCN-STIC 1431 Procedimiento de empleo seguro ArubaOS Controladoras y Puntos de Acceso.

El personal asignado por la empresa adjudicataria deberá conocer y respetar la normativa de seguridad de información de la UBU:

https://www.ubu.es/normativa/normativa-de-administracion-y-gestion-general-de-la-universidad/seguridad-de-la-informacion
así como los procedimientos establecidos por la Universidad que sean de aplicación en el ámbito del contrato.

Será de obligado cumplimiento para el adjudicatario colaborar con el Servicio de Informática y Comunicaciones y aplicar la solución a las vulnerabilidades e incidencias de seguridad que vayan surgiendo.
Se deberán especificar los procedimientos de mantenimiento para proteger el sistema en su conjunto (seguridad en el software empleado, gestión de cambios, gestión de la configuración, gestión de la capacidad, …).
Para la prevención de actualizaciones fallidas, la empresa adjudicataria se asegurará previamente mediante comunicación escrita a los técnicos de la universidad, de la existencia de copias de seguridad convenientemente actualizadas o tomará medidas

adicionales como la creación de ficheros o tablas de respaldo para almacenar la información a modificar, con el fin de poder restaurarla en caso de fallo.

10. PROTECCIÓN DE DATOS

La empresa adjudicataria se compromete a tratar los datos de carácter personal en el ámbito del servicio objeto de este pliego, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la normativa que la desarrolla.

También se compromete a tratar los citados datos, únicamente conforme a las instrucciones de la Universidad de Burgos y a no aplicarlos o utilizarlos con fin distinto al del servicio objeto de este pliego ni a comunicarlos, ni siquiera para su conservación, a otras personas.

ANEXO 1 PUNTOS DE ACCESO (AP) WI-FI

1. Los AP dispondrán de certificado Wi-Fi Certified 6 expedido por la Wi-Fi Alliance.
2. Los AP también dispondrán de certificado Wi-Fi Certified (802.11ax) expedido por la Wi-Fi Alliance.
3. Los AP dispondrán de certificado WPA3 expedido por la Wi-Fi Alliance.
4. Los AP dispondrán de 3 radios independientes (tri-banda) para las bandas de 2.4Gh, 5Ghz y 6Ghz, sin restricciones en la configuración de canales en 5Ghz y 6Ghz sin degradación de rendimiento.
5. Soportaran 1024-QAM para cualquiera de las tres radios y para la de 6Ghz hasta 4096 QAM (o 1024-QAM si no se utilizan extensiones propietarias).
6. Soportará canales 20/40/80/160Mhz en la banda de 6Ghz.
7. Dispondrán de radio BLE y 802.15.4 Zigbee integradas soportando coexistencia avanzada con el servicio IoT.
8. Dispondrán de GPS integrado para servicios de autolocalización y certificación FTM (WFA Location).
9. Dispondrán de puertos USB 5W para modelos de interior.
10. Dispondrá de al menos 2 puertos ethernet NBase-T a 2.5GE (802.bz) o superior.
11. Soportará Jumbo Frames de MTU hasta 9000.
12. Dispondrán de puerto de consola micro USB Serial para modelos de interior o USB-C para modelos de exterior
13. Se podrán alimentar por DC o PoE para equipos de interior.
14. Dispondrán de IPM (Intelligent Power Management).
15. Los modelos serán Plenum rated.
16. Dispondrán de funcionalidad Deep-Sleep Support.
17. Soportarán hasta 37 Resource Units (OFDMA).
18. Número máximo de clientes asociados por radio de 512.
19. Se podrán alimentar por PoE 802.3 AT/BT.
20. Soportarán OFDMA ((Acceso Múltiple por División de Frecuencia Ortogonal).
21. El modelo de antenas integradas dispondrá de 2 antenas Omni Downtilt integradas

ANEXO 2 GESTIÓN CENTRALIZADA EN LA NUBE

Funcionalidades de gestión

1. La solución permitirá una gestión integral centralizada desde una sola consola, con capacidad de implementar una gestión unificada tanto para AP, switches y gateways Wireless/SDWAN.
2. Habilitará visibilidad, integración y orquestación con terceros. Integración vía APIs con sistemas municipales (ej. tarjeta ciudadana), soluciones de seguridad (firewalls, EDR, SIEM) y aplicaciones corporativas.
3. Capacidad para migrar desde versiones anteriores del sistema operativo sin perder configuraciones clave ni interrumpir servicios, y capacidad de mezclar versiones de software en diferentes dispositivos en el mismo entorno, simplificando de esta forma las migraciones.
4. Soportará autorización dinámica de usuarios, permitiendo cambios de roles o políticas sin interrupciones.
5. Dispondrá de funcionalidad de supervivencia: en caso de pérdida de conectividad con la plataforma central, los dispositivos (AP) podrán mantener operativo el servicio sobre la configuración local.

Radiofrecuencia, optimización e inteligencia

6. Funcionalidad de escaneo del entorno radioeléctrico para detección de interferencias y adaptación de parámetros de RF dinámicamente.
7. Implementación de algoritmos internos de detección de anomalías, correlación de eventos y análisis de causa raíz para reducir tickets operativos.
8. Motor de optimización de radiofrecuencia que ajuste canales, potencias y otros parámetros automáticamente.
9. Mecanismo que mueve clientes entre puntos de acceso cuando la conexión se vuelve subóptima, evitando lo que se conoce como “client stickiness” o clientes pegajosos.
10. Mecanismos de reserva de recursos radioeléctricos (división dinámica del medio) destinados a garantizar latencias mínimas en aplicaciones críticas (como voz/video).

Itinerancia, experiencia de usuario y servicios de red

11. Funcionalidad de itinerancia optimizada con balanceo de carga entre APs para distribuir clientes uniformemente.
12. Visualización y monitoreo del rendimiento de aplicaciones de voz y vídeo, con métricas de calidad.
13. Funcionalidad de autenticación automática de invitados mediante credenciales de redes móviles o similares, facilitando la extensión de cobertura sin infraestructura extra.
14. Funcionalidad de descubrimiento y compartición de dispositivos en red (impresoras, proyección, multimedia) mediante proxy multicast / servicios de red local.
15. Movimiento (roaming) fluido entre puntos de acceso con cambio automático hacia AP con mejor calidad de señal.

Infraestructura Cloud

16. Se contará con una plataforma de gestión en entorno Cloud que permita gestionar desde una nube externa a la infraestructura del Ayuntamiento todo el equipamiento de las diferentes sedes sobre un panel de control único.
17. La solución debe implementar una arquitectura de instancias distribuidas para garantizar máxima disponibilidad.
18. El servicio SaaS incluirá cualquier mantenimiento necesario en la plataforma de gestión y permitirá disponer siempre de las mejoras desarrolladas en el servicio y actualizaciones de seguridad.

Funcionalidad de monitorización

19. La plataforma habilitará un panel de control único que permita gestionar desde un único punto la infraestructura de toda red, simplificando las tareas de supervisión y gestión de la red.
20. Permitirá gestionar AP, switches, y gateways SD-WAN tanto físicos como virtuales, desde una única interfaz.
21. Debe habilitar la visión extremo a extremo, de la comunicación de los dispositivos de usuario final conectados siguiendo el flujo completo: Dispositivo -> Punto de

Acceso -> Switch -> Gateway -> Túneles SD-WAN –> Gateway terminador del túnel. Permitiendo detectar y resolver problemas de conectividad de forma sencilla y rápida.

22. Debe permitir mostrar información de los dispositivos finales (PC, tablets, móviles, etc.) conectados a la red incluyendo información de perfilado del dispositivo (SO, tipo de dispositivo, etc.). También debe permitir el etiquetado (tags) de los dispositivos conectados. Y con ello mejorando la visibilidad y control sobre los dispositivos conectados, facilitando la gestión de seguridad y rendimiento.

Funcionalidad de provisión

23. Dispondrá de funcionalidad de aprovisionamiento automático de equipos (AP), sin intervención manual, al conectar dispositivos nuevos mediante Zero Touch Provisioning (ZTP).
24. Debe permitir realizar actualización de firmware de forma remota de los equipos, reduciendo la necesidad de desplazamientos técnicos y mejorando la eficiencia operativa.
25. Debe permitir actualizaciones de firmware en el momento y mediante programación, permitiendo programaciones fuera de horario de oficina buscando el mínimo impacto en el servicio.
26. Debe permitir el despliegue masivo de configuraciones, facilitando la implementación rápida y homogénea en despliegues.
27. Debe disponer de menús autoguiados (wizards) para la configuración de los distintos dispositivos, facilitando el trabajo técnico y minimizando errores de configuración.

Funcionalidad de operación

28. Se valorará que la solución disponga de mecanismos de ayuda a la operación basados en capacidades de analítica inteligente que permita la visualización de métricas de conectividad Wi-Fi, disponibilidad de puntos de acceso y calidad del servicio inalámbrico.
29. Se valorará que disponga de un motor de búsqueda con lenguaje natural que permita localizar fácilmente información sobre clientes, dispositivos e infraestructura de red desde la consola de gestión.

30. Se valorará que incluya capacidades de diagnóstico mediante registros dinámicos que faciliten la recolección y análisis de información de los dispositivos para resolución de incidencias.
31. Proporcionará información de detalle de situaciones anómalas de la red, es decir situaciones no caracterizadas como alarmas ni eventos al uso, permitiendo detectar problemas ocultos.
32. Tendrá capacidad de proponer de manera autónoma modificaciones en la configuración de la red que solucionen las situaciones anómalas.
33. Deberá proporcionar información del estado de la conectividad WI-FI utilizando parámetros como tiempos de asociación, de autenticación, de asignación de dirección por DHCP y de resolución de DNS, facilitando el análisis de rendimiento y mejorando la calidad del servicio.

Mecanismos de disponibilidad

34. Los equipos podrán seguir operando con el 100% de funcionalidades al perder conectividad con la Cloud, para todas las funcionalidades que residan en local.
35. Se deberá mantener una interfaz de control y configuración en caso de caída de la conexión con la plataforma de configuración Cloud. Se podrán efectuar cambios de configuración en local que luego serán sincronizados con la solución Cloud de forma automática.
36. Los dispositivos (AP) dispondrán de una interfaz de gestión local incluso después de cesar la suscripción Cloud, pudiéndose mantener las configuraciones al 100% (para aquellas funcionalidades disponibles en local).

Facilidades de configuración WI-FI

37. Se podrán configurar SSID para ser radiados en las bandas de 2,4GHZ, 5GHz y 6GHZ.
38. Existirá la posibilidad de configurar en la plataforma la programación de SSID para habilitarlos en un determinado horario predefinido.
39. La solución Cloud incorporará portales cautivos Wi-Fi personalizados que permitan integrar el acceso de invitados mediante:

a) Solución de auto-registro con redes sociales, incluyendo Facebook, Twitter, Google y LinkedIn.
b) Se podrá realizar auto-registro de usuarios que requieran verificación de la cuenta. Esta verificación podrá ser mediante email o SMS.
c) Se incorporará una pasarela de SMS para el envío de credenciales por mensaje dentro de la solución Cloud sin coste adicional por envío de SMS
d) Permitirá incorporar funcionalidades de MAC-Caching

40. Se podrán mantener diferentes versiones de firmware de los AP en diferentes sedes.
41. Se podrá realizar cambios de firmware a versiones anteriores siempre que se deseen, incluso disponer de versiones futuras para probar nuevas funcionalidades.

Funcionalidades de seguridad

42. La plataforma Cloud dispondrá de mecanismos para el control de la seguridad de la red en cuanto a detección de eventos de intrusiones y AP sospechosos en entornos WI-FI (Rogue AP).
43. Los AP WI-FI y gateways llevarán incluidas capacidades de firewall de nivel 7. Estas capacidades de firewall se podrán configurar desde la plataforma Cloud.
44. Las sesiones asociadas al firewall integrado en los AP y los gateways se podrán monitorizar desde la plataforma Cloud.
45. Se dispondrá de mecanismos de clasificación y contención de contenidos Web.
46. Se dispondrá de un Filtrado URL según las políticas de configuración que se decidan establecer y totalmente personalizables.
47. Permitirá acceso controlado por categoría web, aplicaciones, destinos y reputación web.
48. Permitirá control de ancho de banda, tanto por SSID como por usuario.
49. Permitirá registro de logs y exportado a syslogs.
50. Dispondrá de un histórico de los cambios efectuados en la configuración por diferentes usuarios, para poder realizar un seguimiento específico.
51. Permitirá reporting e informes de acceso.
52. Permitirá alertas del sistema.
53. Permitirá aislar a los clientes Wi-Fi para que no puedan tener conectividad entre sí en cada SSID.

54. Permitirá disponer de capacidades IDS/IPS en los gateways, configurables desde la plataforma Cloud.

La Jefa del Servicio de Informática y Comunicaciones