SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

AMPLIACIÓN DE LA INFRAESTRUCTURA DE LA RED WIFI DE LA UNIVERSIDAD DE ALCALÁ

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Universidad de Alcalá

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

ÍNDICE

Universidad de Alcalá

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

1. OBJETO DEL CONTRATO

El objeto de este contrato es la adquisición de equipamiento para la infraestructura de la red WiFi de la Universidad de Alcalá que permita ampliar la cobertura de red inalámbrica proporcionada a la comunidad universitaria, así como mejorar los sistemas de autenticación y accounting de los usuarios conectados.

2. RED WiFi DE LA UNIVERSIDA DE ALCALÁ

La infraestructura WiFi de la Universidad, está basada en su totalidad en la solución Aruba Wireless LAN del fabricante ARUBA y está compuesto por controladoras inalámbricas en versión 8 con Mobilty Master y cerca de 800 puntos de acceso inalámbrico (APs) de distintos modelos distribuidos de forma equitativa entre las controladoras.

Cada uno de los APs cuenta con las siguientes licencias cargadas en las controladoras:

- Licencia de AP, requerida para que cada AP operativo conectado a LAN, en malla o remoto anuncie al menos un BSSID (AP virtual).
- Licencia de Firewall, que permita a un AP operativo la identificación inteligente de aplicaciones, la gestión y los controles de tráfico basados en políticas o los firewalls de usuario con estado.
- Licencia de Protección de Radio Frecuencia, que permita al AP realizar funciones de análisis de espectro y protección contra intrusiones inalámbricas (WIP).

La mayoría de los APs se encuentran instalados en interior, haciendo uso de sus correspondientes soportes. Los APs se conectan a electrónica de red de área local, en puertos que soportan PoE+ y con una velocidad de 1Gbps.

Como herramienta de monitorización y gestión de la red inalámbrica, los Servicios Informáticos de la Universidad utilizan AirWave, con capacidad de gestión de hasta 1000 dispositivos.

Para la gestión de invitados y redes de congresos y accounting de conexiones se utiliza el software ClearPass Policy Manager.

La Universidad de Alcalá participa en la iniciativa eduroam de RedIRIS y GEANT y permite el acceso a su red inalámbrica a los usuarios de cualquier organización afiliada a dicha iniciativa. Ofrece así un SSID eduroam, al que se puede conectar cualquier usuario con credenciales y configuración específica en sus dispositivos

Para la autenticación de usuarios se utilizan dos servidores Freeradius virtuales en configuración activo-pasivo.

Todas estas herramientas y software se encuentran desplegados en servidores virtuales dentro del entorno VMWare propio de los Servicios Informáticos.

3. EQUIPAMIENTO A SUMINISTRAR

3.1. Controladora inalámbrica

Se debe suministrar una controladora inalámbrica, que deberá ser completamente compatible, interoperable y funcional con todos los elementos hardware y software de la infraestructura WiFi ARUBA existente.

La controladora inalámbrica se suministrará con fuente de alimentación redundante y dos SFP-10GE-SR 10GBASE-SR SFP+ con conectores LC.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

Junto a esta controladora se deben suministrar, además, las siguientes licencias de funcionamiento:

- 218 licencias de AP, requerida para que cada AP operativo conectado a LAN, en malla o remoto anuncie al menos un BSSID (AP virtual).
- 218 licencias de Firewall, que permita a un AP operativo la identificación inteligente de aplicaciones, la gestión y los controles de tráfico basados en políticas o los firewalls de usuario con estado.
- 218 licencias de Protección de Radio Frecuencia, que permita al AP realizar funciones de análisis de espectro y protección contra intrusiones inalámbricas (WIP).

Los servicios asociados al suministro de esta controladora y licencias son los siguientes:

- Soporte PBS (Partner Branded Services) por parte de fabricante por un año.
- Garantía extendida de integrador hasta el 31 de julio de 2026.
- Servicios de integrador para la instalación y configuración de la controladora en clúster con las controladoras ya existentes.

Las características técnicas mínimas de este equipamiento se especifican en el punto 4 del presente pliego.

3.2. Sistema de autenticación, autorización y accounting (AAA)

Como parte de la evolución tecnológica de la red WiFi, se contempla la sustitución del sistema actual de AAA basado en tecnología FreeRadius por un sistema de alta disponibilidad que tenga como uno de los elementos el servidor ClearPass existente.

Se deberá suministrar y configurar un sistema de Autenticación, Autorización y Accounting, en formato virtual VMWare, completamente compatible e interoperable con el servidor ClearPass existente, también en formato virtual VMWare, que permita la configuración en clúster de ambos sistemas.

Se deberá integrar en la infraestructura ‘eduroam’, y por tanto en la jerarquía de radius ‘eduroam’.

Así mismo, se deberán incluir licencias Access para 10.000 usuarios concurrentes para el clúster formado por el sistema de AAA a suministrar y ClearPass existente. Las licencias deben compartirse por los elementos del clúster AAA - ClearPass. Estas licencias deberán ser permanentes, sin que se requiera su renovación temporal.

Los servicios asociados al suministro de este sistema y licencias son los siguientes:

- Soporte PBS (Partner Branded Services) por parte de fabricante por un año.
- Garantía extendida de integrador hasta el 31 de julio de 2026.
- Servicios de integrador para:
    - Configuración e integración con la instancia virtual ClearPass existente en modo clúster.
    - Carga de las licencias de usuario en el clúster AAA - ClearPass.
    - Configuración del clúster como sistema de autenticación, autorización y accounting de la red WiFi de la UAH, dentro de la jerarquía eduroam, de tal forma que sustituyan a los servidores FreeRadius existentes.
    - Configuración de autenticación radius, TACACS o equivalente, de los usuarios de administración del clúster de AAA.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

Las características técnicas mínimas de este equipamiento se especifican en el punto 4 del presente pliego.

3.3. Puntos de acceso inalámbricos

Se suministrarán 10 puntos de acceso (APs) WiFi 6E de interior de rendimiento moderado, que incluirán los correspondientes anclajes y/o soportes necesarios para su fijación en pared.

Los puntos de acceso suministrados deberán ser completamente compatibles, interoperables, intercambiables y funcionales con todos los elementos hardware y software de la infraestructura WiFi ARUBA existente.

Deberán contar con garantía durante la vida útil por parte del fabricante.

La instalación correrá a cargo de la Universidad, por lo que no es objeto de este contrato.

Las características técnicas mínimas de este equipamiento se especifican en el punto 4 del presente pliego.

Los servicios asociados al suministro de este sistema y licencias son los siguientes:

- Soporte software por parte del fabricante por 1 año.
- Garantía extendida de integrador hasta el 31 de julio de 2026.
- Servicios de integrador para un estudio de cobertura inalámbrica que permita la correcta ubicación de los puntos de acceso suministrados y optimización de la infraestructura existente. Las características de este servicio son las siguientes:
    - Estudio de cobertura WiFi on-site, en 29 edificios del campus de la UAH.
    - Cobertura total de los espacios indicados en la banda de 5 GHz.
    - Se realizará en todas las zonas de interior de los edificios, a excepción de las zonas de parking e instalaciones (transformadores, calderas, etc.). También en las zonas de exterior de los patios del edificio de San Ildefonso.
    - Cobertura RF mayor o igual que -65dBm.
    - Según el estudio de cobertura se determinarán las carencias de cobertura y capacidad a solventar y la posible instalación de nuevos APs o modificación de ubicación de los ya instalados, teniendo que cuenta que:
        - Con estas propuestas de debe conseguir cobertura 100% de los edificios en la banda de 5GHZ.
        - Se debe garantizar que la infraestructura inalámbrica permite un número de conexiones que sea el doble de la capacidad de usuarios de los espacios.
        - Se deberá proponer el modelo de AP a instalar o sustituir en cada caso.
    - Los estudios se presentarán a los Servicios Informáticos de la universidad, para acordar conjuntamente la disposición más adecuada en cada edificio.
    - Elaboración y entrega de la documentación (informes) con resultados de los estudios, que deberán incluir datos tales como:
        - Reportaje gráfico.
        - Listado de APs y SSID radiados.
        - Mapas de calor (nivel de señal y cobertura, señales de ruido (interferencias), relación señal a ruido (SNR), análisis de espectro, etc.).

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

        - Conclusiones y recomendaciones tales como necesidad de nuevos APs (tanto en zonas que se detecte ausencia de señal o deficiencias en la misma), cableado adicional, medidas correctoras y redistribución de los APs.
    - Los edificios en los que se debe realizar este estudio son los siguientes: Ambientales, Arquitectura, Colegio de Caracciolos, Ciencias, Colegio de León, Colegio Irlandeses, CRAI, Derecho, Documentación, Económicas, Enfermería, Farmacia, FGUA, Filosofía, Genética, Jardín Botánico, Magisterio Medicina, Politécnico, Polivalente, Química Fina, Rectorado San Ildefonso, Rectorado San Pedro y San Pablo, Rectorado Santo Tomás, San Bernardino, Servicio de Deportes, y Colegio de Trinitarios
    - El estudio se realizará en horario laboral de lunes a viernes.
    - Se proporcionará fichero comprimido de los planos de los edificios para la estimación económica de este servicio.
    - Los estudios de cobertura se llevarán a cabo con software compatible con Ekahau. Los ficheros de trabajo de los estudios se entregarán a la universidad.

4. CARACTERÍSTICAS TÉCNICAS

Las características técnicas mínimas del equipamiento a suministrar se indican a continuación.

4.1. Controladora inalámbrica

- Rendimiento y capacidad
    - APs máximos -> 512
    - RAPs máximos -> 512
    - Dispositivos concurrentes máximos -> 16.384
    - VLANs -> 4.094
    - Túneles GRE concurrentes (BSSIDs de Sistema) -> 8.192
    - Puertos en Túnel concurrentes -> 8.192
    - Sesiones IPSec concurrentes -> 16.384
    - Sesiones fallback SSL concurrentes -> 8.192
    - Sesiones de Firewall Activas concurrentes -> 2.015.291
    - Throughput alámbrico (grandes paquetes) -> 20Gbps
- Interfaces e indicadores
    - Cuatro puertos 10GBASEX (SFP+)
    - Un USB 2.0
    - Consola (RS-232) RJ-45 o mini-USB
    - LEDs LINK/ACT y status
    - LEDs management/status
    - Panel LCD y botones de navegación
    - Dimensiones
    - (H) 4.4 cm x (W) 44.5 cm x (D) 44.5 cm (1.75” x 17.5” x 17.5”)
    - Peso (con una fuente AC instalada) 7.45 kg (16.43 lbs)
- Características Ambientales
    - Rango de temperatura de operación: 0° C a 40° C
    - Humedad de operación: 5% a 95% sin condensación
    - Rango de temperatura de almacenamiento: -40° C a 70° C
    - Humedad de almacenamiento: 5% a 95% sin condensación

    - Altura de operación: 10,000 pies
    - Ruido acústico (con fuente AC): 46.9 dBA
        - Sound power per ETSI 300 753 de acuerdo con ISO 7779
- Especificaciones de la Fuente de Alimentación
    - Fuente de alimentación AC de 350 watts
    - Voltaje de entrada AC: 100 VAC a 240 VAC
    - Corriente de entrada AC: 5-2.5A
    - Frecuencia de entrada AC: 50-60 Hz
    - Peso: 2.8 lbs (1.3 kg)
    - Consumo máximo de potencia 125 watts
- Cumplimiento Regulatorio y de Seguridad
    - FCC Part 15 Class A CE
    - Industry Canada Class A
    - VCCI Class A (Japan)
    - EN 55022 Class A (CISPR 22 Class A), EN 61000-3,
    - EN 61000-4-2, EN 61000-4-3, EN 61000-4-4,
    - EN 61000-4-5, EN 61000-4-6, EN 61000-4-8,
    - EN 61000-4-11, EN 55024, AS/NZS 3548
    - UL 60950, EN60950
    - CAN/CSA 22.2 #60950
    - CE mark, cTUVus, CB, C-tick, Anatel, NOM, MIC
- Información SKU Regulatoria
    - ARCN0101

4.2. Sistema de autenticación, autorización y accounting (AAA)

- Arquitectura:
    - El sistema estará disponible en versión máquina virtual compatible con VMWare para facilitar su despliegue.
    - La solución a configurar debe ser totalmente redundada para soportar estados degradados en caso de fallo de una máquina virtual.
    - Todos los nodos en la arquitectura de alta disponibilidad deben funcionar de forma activo-activo.
    - El escalado y crecimiento debe ser de forma horizontal de tal forma que para aumentar la capacidad global solo hagan falta añadir nodos adicionales.
    - Deberá existir un único nodo de configuración del sistema y deberá sincronizar la configuración al resto de equipos.
    - El sistema deberá incorporar mecanismo de encriptado de datos internos mediante Linux Unified Key Setup (LUKS) mediante AES-256.
- Compatibilidades:
    - El Sistema debe poseer de mecanismos de perfilado de perfilado de dispositivos. Para el perfilado se deberán usar al menos los siguientes mecanismos:
        - Activos: NMAP, WMI, SSH, SNMP
        - Pasivos: MAC-OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFlow, Span Port, HTTP User-Agent, IF-MAP
        - Otros: Agente Posture, integración con soluciones MDM, certificados.
    - La solución debe contar con firmas de profiling incorporadas. En cualquier caso, se podrán realizar actualizaciones de las mismas en función de los dispositivos que se conecten.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

- El sistema detectará automáticamente posibles conflictos en el perfilado y marcará los Endpoints si detecta incongruencias.
- El sistema deberá utilizar protocolos estándar que garanticen su compatibilidad con distintos equipos de acceso (switches, routers, firewalls, controladores WLAN, terminadores VPN) de distintos fabricantes.
- El sistema deberá realizar descubrimiento y perfilado de dispositivos sin necesidad de sondas o equipos adicionales en sedes remotas.
- El sistema debe poderse integrar en más de un dominio corporativo para realizar consultas en el Directorio Activo.
- Se deberán soportar integraciones con sistemas de entidades externas:
  - Microsoft Active Directory
  - RADIUS
  - Directorios LDAP
  - MySQL, Microsoft SQL, PostGRES y Oracle 11g ODBC-compliant SQL server
  - Servidores de Token
  - Kerberos
  - Microsoft Azure Active Directory
  - Google G Suite
  - Built-in SQL Store, static host-list
- Soporte de autenticaciones mediante 802.1X, autenticación MAC y con portal cautivo.
- Soporte de autenticación basado con SNMP con switches que no soportes protocolos RADIUS.
- Se deberán poder realizar simulaciones de políticas de seguridad antes de su implantación.
- Soporte de servicios AAA (Authentication, Authorization and Accounting) con los métodos de autenticación más utilizados en la industria:
  - RADIUS, RADIUS CoA, TACACS+, Web authentication, and SAML v2.0
  - EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
  - PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public)
  - TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
  - EAP-TLS
  - PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5
  - Wireless and wired 802.1X and VPN
  - OAuth2
  - Microsoft NAP and NAC
  - Windows machine authentication
  - Online Certificate Status Protocol (OCSP)
  - SNMP generic MIB, SNMP private MIB
  - Common Event Format (CEF), Log Event Extended Format (LEEF)
- Posibilidad de separar los procesos de Autenticación y Autorización – cada proceso deberá poder utilizar bases de datos distintas.
- Se deberá soportar RadSec para comunicación segura entre el RADIUS y los NAS.
- Se deberá soportar el envío de CoA (Change of Authentication) mediante atributos RADIUS estándar a equipos Wired y Wireless. No será necesario proporcionar credenciales de administración para ejecutar el CoA.
- El sistema tendrá funcionalidades de Autorización del acceso en función de características como pertenencia a un grupo de usuarios, tipo de dispositivo móvil, aplicación utilizada, localización del dispositivo, estado de salud (health check) del dispositivo, etc.
- El sistema implementará los siguientes estándares RFC
  - RFC 2246 The TLS Protocol Version 1.0
  - RFC 2248 Network Services Monitoring MIB

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

  - 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
- El sistema soportará la gestión automática de claves de acceso para que puedan controlar el acceso de dispositivos mediante SSID con WPA2 y claves pre-compartidas (PSK) diferentes (MPSK). Esta funcionalidad podrá estar destinada a dispositivos IoT que acceden por un mismo SSID pero que no disponen de suplicante 802.1X y requieren un acceso controlado.

- Acceso de invitados con portales cautivos de acceso:
  - Se podrá realizar el registro de dispositivos mediante portales cautivos, orientado a Guest, soluciones BYOD y gestión de dispositivos.
  - El sistema incluirá la posibilidad de generar diferentes portales cautivos para la autenticación de invitados compatible con las soluciones WLAN más habituales de los distintos fabricantes de la industria.
  - 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: email, 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 IT.
  - El tiempo de expiración de las cuentas de invitados deberá ser configurable.
  - Los portales cautivos permitirán personalizar el look&feel de forma completa, con posibilidad de adaptación del código HTML completo y de las hojas de estilo CSS.
  - Los formularios de acceso de invitados podrán personalizarse en todos sus campos con al menos las siguientes capacidades mínimas:
    - 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, y cualquier opción adicional. El contenido de estos campos será personalizable.
    - Generación de portales HTML de distinto tamaño en función del tamaño y resolución de las pantallas de los dispositivos móviles. El portal deberá redimensionarse automáticamente en función del dispositivo que lo visualiza.
    - Posibilidad de incluir todo de tipo de contenido multimedia en el portal: imágenes, audio, video, etc… que varíe de forma dinámica según patrones establecidos. Este

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

contenido podrá referenciarse a enlaces externos o podrá ser incluido en el propio Sistema. No existirá limitación de imágenes o contenidos que se podrán incluir.
    - El portal proporcionará informes de actividad relativa al tráfico de invitados: número de visitas, contenido multimedia mostrado, numero de SMS enviados con credenciales, etc…
    - El portal permitirá integrarse con soluciones de doble factor de autenticación.
    - Se podrán realizar integraciones con sistemas de terceros mediante OpenAuth para permitir 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 SI (ONTSI).
    - Los portales de acceso permitirán integración con redes sociales como Facebook, Facebook WiFi, Google Plus, Twitter, Instagram, LinkedIn, etc.
- Health-Check:
    - La solución NAC deberá incorporar mecanismos para realizar el control de salud de los dispositivos que se conecten a la red.
    - Se deberán soportar agentes pesados (que requieren instalación) y agentes solubles (agentes que se ejecutan sin quedar permanentes en los endpoints).
    - Se soportará health-check mediante funcionalidad “agentless” donde no se requiera la instalación de un agente para entornos Windows.
    - La solución deberá proporcionar un workflow sencillo para que los usuarios puedan provisionarse cualquiera de los dos agentes. La provisión se realizará mediante portales cautivos configurables.
    - El chequeo de salud deberá permitirse para los sistemas operativos mediante agente: Windows, Linux y MacOS.
    - El agente de Linux soluble estará soportado en CentOS, Fedora, RHEL y SUSE
    - Este agente comprobará el estado y actualización de antivirus, antispyware, firewalls, etc…y proporcionará instrucciones de remediación en caso de que el dispositivo viole las políticas corporativas.
    - La información de estado proporcionada por el agente deberá de poder ser consultada en tiempo real.
    - El agente tendrá la capacidad de detener o arrancar procesos internos de los dispositivos en caso de ser necesario.
    - El agente tendrá acceso a las variables de registro de los dispositivos y podrá agregar o eliminar variables en caso de ser necesario.
    - Se valorará que el agente ligero NAC realice comprobaciones avanzadas como detección de programas P2P y utilización de llaves USBs como dispositivos de almacenamiento.
    - En caso de dispositivos corporativos se soportará el control del health-check mediante WMI sin necesidad de agente.
- Gestión de dispositivos Móviles:
    - El sistema proporcionará una infraestructura PKI interna que permita generar credenciales específicas de para dispositivos móviles que sirvan para autorizar estos dispositivos en la red (certificados digitales).
    - La PKI interna permitirá configurarse como Root-CA, Intermediate-CA, Imported-CA o Registration Authority.
    - Debe ser compatible con los dispositivos más habituales: iOS (Apple iPad, iPhone), Android, MacOS X, Windows Mobile, Windows 10.
    - Las credenciales utilizadas para los dispositivos móviles permitirán controlar el acceso de estos dispositivos a la red y denegarlo en caso de robo o pérdida del dispositivo.
    - Se valorará la capacidad del sistema para configurar de manera automática el suplicante 802.1X de los dispositivos móviles.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

- Se valorará la capacidad del sistema para 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.
- Se valorará que la generación y entrega de credenciales para dispositivos móviles suponga una carga de trabajo mínima para el departamento de IT.
- Se valorará que cualquier empleado pueda realizar el proceso de autenticación y autorización de dispositivos móviles sin necesidad de ayuda del departamento de IT.
- Se valorará el empleo de más de un método de detección e identificación de los dispositivos móviles, para evitar la suplantación de identidades (Device Profiling).
- El sistema tendrá la capacidad de utilizar las credenciales de autenticación de red (802.1X) para autenticar también las sesiones de las aplicaciones móviles.
- Los certificados emitidos podrán ser gestionados por un administrador y filtrados por usuario y dispositivos para su revisión, eliminación o revocación.
- Los usuarios podrán disponer de un acceso seguro para conocer los dispositivos que tienen asociados un certificado y revocar/eliminarlos de forma personalizada. Este acceso será configurable y opcional para los usuarios.
- Se podrá limitar el número de dispositivos que pueden disponer de certificado para cada usuario corporativo.

- Integraciones:
  - Se podrán realizar integraciones con terceros. El sistema debe contar con posibilidad de dichas integraciones de manera flexible sin intervención del Fabricante.
  - Se podrá configurar integraciones con terceros mediante consultas http/https para el intercambio de información.
  - El sistema deberá poder exportar a sistemas de terceros información contextual de los usuarios autenticados: username, dispositivo usado, punto de conexión, etc.
  - El sistema soportará la recepción de eventos vía Syslog para ejecutar acciones sobre la infraestructura de acceso, desconectando usuarios o cambiándoles de VLANs.
  - Se deberá soportar la integración con sistemas MDM para recibir información sobre los dispositivos enrolados en dichas plataformas. Se deberá poder comprobar esta información para crear una política de acceso personalizada.
- Otros:
  - La solución NAC debe contar con las siguientes certificaciones de Seguridad:
    - FIPS 140-2
    - Extended Package for Authentication Servers Version 1.
    - Collaborative Protection Profile for Network Devices Version 1.0
  - El sistema debe contar con un sistema de reporting integrado para generar informes programados y bajo demanda sobre la red, usuarios, dispositivos y autenticaciones.
    - Los informes podrán ser personalizados en cuanto a la fecha y al contenido.
    - Se deberán poder hacer informes bajo demanda de autenticaciones satisfactorias y fallidas en periodos de tiempo limitados.
    - Se admitirán filtros en los informes para establecer resultados en función de cualquier atributo RADIUS: NAS, fuente de autenticación, estatus, etc.
    - Se deberán poder generar dos tipos de informes:
      - Informe PDF de alto nivel con información básica y agregada mediante gráficas.
      - Informe con los datos en bruto en formato CSV con los campos personalizables.
    - Los informes podrán generar notificaciones a direcciones de correo electrónico o mediante SMS.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

4.3. Puntos de acceso inalámbricos

- Especificaciones de radio WiFi
  - Tipo de AP:
    - Uso en interiores, radio tri-banda, 2,4 GHz, 5 GHz y 6 GHz. 802.11ax 2x2 MIMO
  - Radio de 6 GHz:
    - Dos MIMO de un solo usuario (SU) de secuencia espacial para una velocidad de transmisión de datos inalámbrica de hasta 2,4 Gbps con dispositivos cliente 2SS HE80 802.11ax.
  - Radio de 5 GHz:
    - Dos MIMO de un solo usuario (SU) de secuencia espacial para una velocidad de transmisión de datos inalámbrica de hasta 1,2 Gbps con dispositivos cliente 2SS HE80 802.11ax.
  - Radio de 2,4 GHz:
    - Dos MIMO de un solo usuario (SU) de secuencia espacial para una velocidad de transmisión de datos inalámbrica de hasta 574 Mbps con dispositivos cliente 2SS HE40 802.11ax.
  - Máxima cantidad de dispositivos cliente asociados:
    - Hasta 256 dispositivos cliente asociados por radio.
  - Máxima cantidad de BSSID:
    - 16 BSSID por radio (limitada a 8 para la banda de 6 GHZ).
  - Bandas de frecuencia admitidas (se aplican restricciones específicas de cada país):
    - 2,400 a 2,4835 GHz.
    - 5,150 a 5,250 GHz.
    - 5,250 a 5,350 GHz.
    - 5,470 a 5,725 GHz.
    - 5,725 a 5,850 GHz.
    - 5.850 a 5.895 GHz
    - 5.925 a 6.425 GHz
    - 6.425 a 6.525 GHz
    - 6.525 a 6.875 GHz
    - 6.875 a 7.125 GHz
  - Dynamic frequency selection (DFS) optimiza el uso del espectro RF disponible en la banda de 5 GHz
  - Canales disponibles:
    - Depende del dominio normativo configurado.
  - Tecnologías de radio compatibles:
    - 802.11b: Espectro ensanchado por secuencia directa (SDSS).
    - 802.11a/g/n/ac: Multiplexación por división de frecuencias ortogonales (OFDM).
    - 802.11ax: acceso múltiple por división de frecuencia ortogonal (OFDMA)* con hasta 8 unidades de recursos (37 para la radio de 6GHz)
  - Tipos de modulación compatibles:
    - 802.11b: BPSK, QPSK, CCK.
    - 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM.
    - 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM.
    - 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.

- Compatibilidad con 802.11n de alto rendimiento (HT):
  - HT20/40.
- Compatibilidad con 802.11ac de muy alto rendimiento (VHT):
  - VHT20/40/80.
- Compatibilidad con 802.11ax de alta eficiencia (HE):
  - HE20/40/80/160.
- Velocidades de datos admitidas (Mbps):
  - 802.11b: 1, 2, 5,5, 11.
  - 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54.
  - 802.11n: 6,5 a 300 (MCS0 a MCS15, HT20 a HT40), 400 con 256-QAM.
  - 802.11ac: 6,5 a 867 (MCS0 a MCS9, NSS = 1 a 2, VHT20 a VHT80), 1083 con 1024-QAM.
  - 802.11ax (2,4 GHz): 3,6 a 574 (MCS0 a MCS11, NSS = 1 a 2, HE20 a HE40).
  - 802.11ax (5 GHz): 3,6 a 1,201 (MCS0 a MCS11, NSS = 1 a 2, HE20 a HE80).
  - 802.11ax (6GHz): 3.6 a 2,402 (MCS0 to MCS11, NSS = 1 a 2, HE20 a HE160)
- Agregación de paquetes de 802.11n/ac:
  - A-MPDU, A-MSDU.
- Potencia de transmisión:
  - Configurable en incrementos de 0,5 dBm.
  - Potencia máxima (combinada, total conducida) de transmisión (limitada por los requisitos reglamentarios locales):
    - Banda de 2,4 GHz, 5 GHZ, 6 GHz: +21 dBm (18 dBm por cadena).
  - Nota: Los valores de potencia de transmisión conducida excluyen la ganancia de la antena. Para conocer la potencia total de transmisión (PIRE), añada la ganancia de la antena.
- Advanced Cellular Coexistence (ACC) minimiza el impacto de interferencias de redes celulares
- Ultra Tri-Band (UTB) habilita flexibilidad máxima en la selección del canal de 5 GHz y 6 GHz sin degradación del funcionamiento
- Maximum ratio combining (MRC) para recepción mejorada.
- Cyclic delay/shift diversity (CDD/CSD) para mejora del funcionamiento del downlink RF.
- Space-time block coding (STBC) para incremento de rango y de mejora de recepción
- Low-density parity check (LDPC) para corrección de error eficiente y aumento de velocidad.
- Transmit beam-forming (TxBF) para aumento de la señal
- 802.11ax Target Wait Time (TWT) para dar soporte a usuarios con baja potencia.
- 802.11mc Fine Timing Measurement (FTM) para mejora de la precisión.
- Antenas WiFi
  - Antenas omnidireccionales integradas con inclinación descendente para MIMO 2x2 con ganancia pico de 4.6 dBi en 2.4 GHz, 7.0 dBi en 5 GHz y 6.3 dBi en 6 GHz. Las antenas integradas están optimizadas para AP instalados en el techo con orientación horizontal. El ángulo de inclinación inferior necesario para lograr la máxima ganancia es de aproximadamente 30 a 40 grados.
  - Si se combinan los patrones de cada una de las antenas de las radios MIMO, la ganancia pico del patrón combinado promedio es de 2.9 dBi en 2.4 GHz, 4.9 dBi en 5 GHz y 4.3 dBi en 6 GHz.
- Otras interfaces
  - E0/E1: Dos puertos Ethernet cableado (RJ-45):

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

        - Velocidad de enlace con detección automática (/100/1000/2500BASE-T) y MDI/MDX.
        - La velocidad de 2,5 Gbps es compatible con las especificaciones NBase-T y 802.3bz.
        - PoE-PD: PoE de 48 VCC (nominal) 802.3at/bt (Clase 4 o superior).
        - Ethernet de bajo consumo (EEE) de 802.3az.
        - Soporte a Link aggregation (LACP) entre ambos puertos de red para redundancia y aumento de capacidad.
    - Interfaz de alimentación de CC:
        - 12 Vcc (nominal, +/- 5 %), acepta un conector circular central positivo de 2,1 mm/5,5 mm con una longitud de 9,5 mm.
    - Interfaz de host USB 2.0 (conector tipo A):
        - Capacidad de suministrar hasta 1 A/5 W a un dispositivo conectado.
    - Radio Bluetooth de baja energía (BLE5.0) y Zigbee (802.15.4):
        - BLE: hasta 5 dBm de potencia de transmisión (Clase 1) y -100 dBm de sensibilidad de recepción (125 Kbps).
        - Zigbee: hasta 5 dBm de potencia de transmisión y -97 dBm de sensibilidad de recepción (250 Kbps)
        - Antena omnidireccional integrada de polarización vertical con inclinación descendente de unos 30 a 40 grados y ganancia pico de 3,0 dBi.
    - Receptor GNSS L1 (1575.42 MHz) para soporte a GPS, Galileo, GLONASS y BeiDou.
        - Sensibilidad de recepción: -160dBm (tracking)
        - Antena integrada omnidireccional inclinación descendente de unos 30 a 40 grados y ganancia pico de 3,6 dBi.
    - Advanced IoT Coexistence (AIC) permite operación concurrente de múltiples radios en la banda de 2.4 GHz
    - Built-in Trusted Platform Module (TPM) para seguridad mejorada.
    - Indicadores visuales (LED multicolores):
        - Para estado de sistema y radio.
    - Botón de reinicio:
        - Restablecimiento a valores de fábrica, control del modo LED (normal/apagado).
    - Interfaz de consola en serie:
        - Conector físico USB micro B.
    - Ranura de seguridad:
        - Ranura de seguridad Kensington.
    - Función de apagado y recuperación automática térmica.
- Fuentes de energía y consumo energético
    - El AP admite energía directa de CC y energía a través de Ethernet en los puertos E0 y E1.
    - Cuando las fuentes de energía CC y PoE están disponibles, la energía de CC tiene prioridad sobre las unidades PoE.
    - Cuando el PoE está disponible en ambos puertos, cualquiera de los puertos puede ser configurado como fuente principal.
    - Cuando esté alimentado por CC o PoE 802.3bt (Clase 5), el AP funcionará sin restricciones.
    - Cuando esté alimentado por PoE 802.3at (Clase 4) y con la función IPM desactivada, el AP desactivará el puerto USB.
    - No se soporta 802.3af.

    - Con IPM activada, el AP se iniciará en modo sin restricciones, pero puede aplicar restricciones de forma dinámica dependiendo del presupuesto de PoE y de la energía real. Se pueden programar las restricciones de la función y el orden.
    - Máximo consumo de energía en el peor de los casos (con o sin dispositivo USB conectado):
        - Alimentación CC: 20,7 W/ 26,4 W.
        - Alimentación PoE: 23,8 W/ 29,4 W.
        - Suponiendo que el dispositivo USB conectado recibe hasta 5 W.
    - Consumo máximo de energía (en el peor de los casos) en modo inactivo:
        - 8,7 / 14,2 W (CC) o 11,7 / 17,2 W (PoE).
    - Consumo de energía máximo (en el peor de los casos) en el modo de suspensión profunda:
        - 1,1 W (CC) o 1,9 W (PoE)
- Especificaciones mecánicas
    - Información de instalación:
        - Preinstalado un soporte de montaje en la parte posterior del AP. Este soporte se utiliza para fijar el AP a cualquiera de los kits de montaje.
- Especificaciones ambientales
    - Condiciones de funcionamiento
        - Temperatura: 0 °C a +50 °C / +32 °F a +122 °F.
        - Humedad: 5 % a 95 % sin condensación.
        - AP clasificado como plenum para uso en espacios para circulación de aire.
        - Entornos ETS 300 019 clase 3.2.
- Condiciones de almacenamiento:
    - Temperatura: -25 °C a +55 °C / -13 °F a +131 °F.
    - Humedad: 10 % a 100 % sin condensación.
    - Entornos ETS 300 019 clases 1.2.
- Condiciones de transporte:
    - Temperatura: -40 °C a +70 °C / -40 °F a +158 °F.
    - Humedad: hasta 95 % sin condensación.
    - Entornos ETS 300 019 clase 2.3.
- Fiabilidad
    - Tiempo medio entre fallos (MTBF):
        - 520 khrs (59 años) a una temperatura de funcionamiento de +25 C.
- Certificaciones:
    - Clasificación plenum UL2043.
    - Wi-Fi Alliance:
        - CERTIFICADO Wi-Fi a, b, g, n, ac.
        - CERTIFICADO Wi-Fi 6E (ax, 6 GHz).
        - WPA, WPA2 y WPA3 - Enterprise con opción CNSA, Personal (SAE), Enhanced Open (OWE).
        - WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multibanda.
        - Passpoint (versión 2).
    - Bluetooth SIG.
    - Ethernet Alliance (PoE, dispositivo PD, clase 4).
- Garantía
    - Garantía limitada de por vida de hardware por parte del fabricante.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

5. SERVICIOS ASOCIADOS

5.1. Gestor único del servicio

El adjudicatario designará en el plazo de 15 días desde el día siguiente de la firma del contrato un Gestor del Servicio, encargado de la puesta en marcha, supervisión, coordinación y control del servicio, siendo el interlocutor único para los asuntos derivados de la gestión del servicio.

El Gestor único del servicio se encargará, al menos, de:

- Proporcionar la documentación de la solución técnica desplegada, plan de implantación gestión del soporte de integrador
- Definir un modelo de procesos, personalizado y aprobado por el Servicio de Comunicaciones de la UAH, para la prestación de los servicios objeto del contrato al inicio de la ejecución del contrato, en el plazo máximo de un mes desde el día siguiente a la firma. Los procesos por modelar serán al menos los siguientes:
    - Gestión y control de la implantación de la solución.
    - Control de la ejecución del contrato.
    - Gestión y control de la garantía extendida de integrador.
    - Control del Acuerdo de Nivel de Servicio.

  Cada proceso definirá como mínimo los siguientes aspectos: procedimiento, actividades del proceso, roles y responsabilidades, entregables y herramientas de soporte a los procesos.
- Agendar y coordinar una reunión de seguimiento del contrato trimestral, donde se proporcionará a los Servicios Informáticos un informe sobre las posibles incidencias y el cumplimiento del ANS de los últimos tres meses.
- Generar los informes adicionales que le sean solicitados por los responsables del Servicio de Comunicaciones de la Universidad

5.2. Garantía extendida de integrador

La garantía extendida de integrador consistirá en:

- Resolución de incidencias nivel 2, apertura y gestión de tickets de soporte con el fabricante.
- Gestión de la garantía proporcionada por el fabricante para el equipamiento de este contrato, con recogida en las dependencias de la UAH del equipamiento averiado, gestión el reemplazo y devolución del equipo nuevo a la UAH. Todo este proceso debe ser asumido por el contratista sin coste alguno para la UAH.
- Actualizaciones de software de la controladora y sistema de AAA. Estas actualizaciones se deberán realizar al menos una vez al año durante la duración del contrato, siempre y cuando exista una versión estable disponible por los fabricantes, o por recomendación de los fabricantes. Y siempre en el caso de problemas de seguridad o funcionamiento en la versión instalada.

Las actuaciones que deba realizar el adjudicatario sobre el equipamiento objeto de este contrato, se realizarán siguiendo el principio de minimización del impacto. Esto es, preferentemente fuera del horario de 08:00 a 20:00 horas días laborables, y de forma remota siempre que sea posible. En caso de que deban realizarse de forma presencial, no tendrán coste adicional alguno para la UAH.

5.3. Centro de Servicio para la gestión de la garantía extendida de integrador

Se dispondrá de un punto de contacto con el proveedor para la atención de incidencias y solicitudes, que atenderá, registrará y escalará al grupo que corresponda las peticiones iniciadas tanto por personal de Servicios Informáticos de la UAH, como por personal de empresas de servicios de TI autorizados por los Servicios Informáticos. El proceso de gestión de incidencias y solicitudes seguirán esquemas similares a los indicados en ITIL v3.

El canal de contacto principal con el centro de servicios será telefónico, mediante un número sin tarificación adicional para la UAH (coste máximo de llamada a números fijos nacionales) y por correo electrónico.

La cobertura horaria para la comunicación de incidencias por parte de los Servicios Informáticos y del personal de servicios de TI será 24x7x365.

5.4. Acuerdo de Nivel de Servicio (ANS)

La resolución de incidencias, tanto en remoto como on-site, se realizará en cobertura 24x7 la controladora inalámbrica y el sistema de AAA y en cobertura 12x5 (lunes a viernes de 8:00 a 20:00) para los puntos de acceso inalámbricos.

El cumplimiento de los requisitos especificados dentro del presente pliego se regulará por un “Acuerdo de Nivel de Servicio” (ANS). En consecuencia, las tareas correspondientes deberán realizarse ajustándose a los “Indicadores de nivel de servicio (INS)” y “valores objetivos” (VO) detallados a continuación. El adjudicatario, dentro del ámbito de las prestaciones que se regulen por el sistema de ANS, será responsable del cumplimiento de todos los VO establecidos, con independencia de los recursos que para ello tenga que incorporar en cada momento.

El adjudicatario se responsabilizará de que, si existen acuerdos de servicio firmados con sus proveedores de mantenimiento y soporte, previamente autorizados por la UAH, éstos respaldarán los niveles de servicio acordados.

La descripción de categorización de las prestaciones es la que sigue a continuación:

- Críticas: Incidencias en la controladora inalámbrica o en el sistema AAA.
- Ordinarias: Incidencias en los puntos de acceso inalámbricos.

Los indicadores contemplados para este tipo de servicio son los siguientes:

1.- Tiempo de respuesta: Plazo máximo transcurrido desde el momento que la incidencia es detectada o comunicada al adjudicatario y registrada en el sistema de gestión de incidencias y peticiones, hasta que los técnicos de la empresa adjudicataria comienzan a trabajar en la incidencia.

Indicador	Valor objetivo	Valor mínimo de cumplimiento
Plazo máximo de atención en la categoría Crítica	<=2 horas	95%
Plazo máximo de atención en la categoría Ordinaria	<=8 horas	95%

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

Los valores serán contabilizados en los horarios indicados para la cobertura 12x5 o 24x7 según la criticidad del equipamiento. Los valores contabilizados serán los no achacables a la lógica de los propios sistemas de gestión o bien a errores o falta del software base para los que no exista solución conocida en forma de parche o procedimiento documentado.

2.- Tiempo de resolución: Plazo máximo transcurrido desde el momento que la incidencia es detectada o comunicada al adjudicatario y registrada en el sistema de gestión de incidencias y peticiones, hasta que la misma queda resuelta y con el visto bueno de los Servicios Informáticos.

Indicador	Valor objetivo	Valor mínimo de cumplimiento
Plazo máximo de resolución en la categoría Crítica	<=8 horas	95%
Plazo máximo de resolución en la categoría Ordinaria	<=48 horas	95%

6. PRESTACIONES A REALIZAR

Las prestaciones a realizar para conseguir el objeto de este contrato son:

- Designar un Gestor del Servicio, encargado de la supervisión, coordinación y control del servicio.
- Suministro, instalación y configuración de la controladora inalámbrica y del sistema AAA, según las especificaciones de los Servicios Informáticos.
- Suministro de los puntos de acceso inalámbricos.
- Suministro e instalación de las licencias del equipamiento instalado
- Prestación de soporte nivel 2 por parte del adjudicatario.
- Gestión de la garantía y soporte del fabricante.
- Garantía extendida del integrador.

7. SEGUIMIENTO, CONTROL Y SUPERVISIÓN DE LA EJECUCIÓN

Las actividades que se realizarán para el seguimiento, supervisión y control de la ejecución del contrato son las siguientes:

- Nombrar un gestor único del servicio por parte del contratista en el plazo de 15 días desde la fecha de inicio del contrato.
- Entregar en el plazo de quince días naturales desde la fecha de inicio del contrato al Servicio de Comunicaciones de la UAH la certificación profesional activa Experto en ClearPass certificado de Aruba (ACCX) y Experto en Movilidad certificado de Aruba (ACMX), para los técnicos asociados a este contrato, y el certificado como partner GOLD, PLATINUM o GLOBAL PARTNER del adjudicatario por parte del fabricante Aruba.
- Entregar en el plazo de quince días naturales desde la fecha de inicio del contrato al Servicio de Comunicaciones de la UAH la certificación profesional activa de las soluciones presentadas de los técnicos asociados a este contrato, y el certificado como partner del adjudicatario.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

- Definición en un plazo de quince días naturales desde la fecha de inicio del contrato por parte del Gestor del servicio de un modelo de procesos, personalizado y aprobado por el Servicio de Comunicaciones con la UAH, para la prestación de los servicios objeto del contrato.
- Control de la implantación de la solución y control de la calidad de las instalaciones realizadas, así como la toma de medidas en caso de deficiencias.
- Centro de Servicios para la comunicación de incidencias y solicitudes relativas al servicio.
- Reunión de seguimiento trimestral, donde se proporcionará a los Servicios Informáticos un informe sobre las posibles incidencias ocurridas y el cumplimiento del ANS de los últimos seis meses.

8. INSPECCIÓN DE LAS INSTALACIONES Y CONTROL DE CALIDAD

La UAH podrá realizar inspecciones aleatorias al objeto de verificar que los suministros y servicios prestados por el contratista se ajustan a las condiciones estipuladas en el presente pliego.

En el supuesto de que alguno de los elementos analizados mostrase deficiencias o incumplimientos de las características técnicas y de calidad requeridas en este pliego, el contratista deberá retirar esos elementos en el plazo de **TRES DÍAS** hábiles a contar desde la comunicación efectuada por escrito por la UAH y reponerlos en las debidas condiciones en el plazo máximo de **CINCO DÍAS** hábiles a contar desde el día siguiente al de la retirada.

9. TRANSFERENCIA TECNOLÓGICA

Durante la prestación del servicio objeto de este contrato, el adjudicatario facilitará en todo momento a las personas designadas por la UAH a tales efectos, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrolla el servicio, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos, así como información y documentación sobre la solución técnica empleada.

10. PREVENCIÓN DE RIESGOS LABORALES Y COORDINACIÓN DE ACTIVIDADES EMPRESARIALES

Tanto el contratista como las empresas subcontratadas o trabajadores autónomos contratados por esta cumplirán en el desarrollo de sus funciones con los requisitos legales que marca la Ley 31/1995 de Prevención de Riesgos Laborales y con el R.D 171/2004, de coordinación de actividades empresariales, en cada caso.

La empresa contratista informará con suficiente antelación al Servicio de Prevención de la Universidad (servicio.prevencion@uah.es) cada vez que subcontrate trabajos a realizar en la propia Universidad, con otra empresa o trabajador autónomo, indicando la forma de coordinación preventiva establecida entre ellos.

El contratista cumplirá asimismo con el procedimiento de coordinación de actividades empresariales vigente en la UAH en todo aquello que le sea aplicable.

En caso de que un trabajador de la empresa contratista sufra un accidente de trabajo mientras desempeña los servicios contratados por la UAH, la empresa contratista informará asimismo al Servicio de Prevención de la Universidad a la mayor brevedad posible.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

11. MEDIDAS DE PROTECCIÓN AMBIENTAL

El adjudicatario se compromete a respetar la normativa vigente al respecto, ya sea de carácter estatal, autonómica, local o universitaria, en el servicio prestado a la UAH.

[Firmado electrónicamente]

Cargo: Director de los Servicios Informáticos

Firmado digitalmente por
CABRERA SILVA MANUEL - DNI
08966521V
Fecha: 2024.09.05 16:39:30 +02'00'