VICEPRESIDENCIA TERCERA DEL GOBIERNO
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSICIÓN ECOLÓGICA Y EL RETO DEMOGRÁFICO

AEMet
Agencia Estatal de Meteorología

SERVICIOS DE GESTIÓN DE RED PARA LA AGENCIA ESTATAL DE METEOROLOGÍA

PLIEGO DE PRESCRIPCIONES TÉCNICAS (PPT)

FEBRERO 2024

Contenido

1. INTRODUCCIÓN

La Agencia Estatal de Meteorología (AEMET) es una entidad encargada de recopilar, analizar y difundir información relacionada con las condiciones meteorológicas y climáticas. Tanto los servicios de red de área amplia (WAN) como los de red de área local (LAN) son fundamentales para el funcionamiento eficiente de la AEMET y poder llevar a cabo las anteriores funciones. En efecto, y con respecto a los servicios WAN se tiene:

- Intercambio de Datos:

  AEMET necesita compartir datos meteorológicos con otras instituciones, agencias gubernamentales, y organizaciones a nivel regional, nacional e incluso internacional. Una red WAN permite el intercambio eficiente de datos entre diferentes ubicaciones geográficas, lo que es esencial para la colaboración y la toma de decisiones informada.

- Acceso Remoto:

  Dada la naturaleza distribuida de las estaciones meteorológicas automáticas, estaciones meteorológicas aeronáuticas, grupos funcionales de predicción del Sistema Nacional de Predicción, sedes de delegaciones territoriales, centros meteorológicos y el Centro de Proceso de Datos, una red WAN permite el acceso remoto a sistemas y datos. Esto facilita la supervisión y el control centralizado de las operaciones meteorológicas, incluso desde las diferentes ubicaciones alejadas.

- Resiliencia y Redundancia:

  La implementación de una red WAN robusta con redundancia garantiza la disponibilidad continua de servicios meteorológicos incluso en situaciones de fallos o eventos adversos.

Asimismo, y con respecto a los servicios LAN, se tiene:

- Recopilación de Datos en Tiempo Real:

  Las estaciones meteorológicas locales, sensores y equipos de medición están conectados a la LAN para recopilar datos en tiempo real. Esto permite una supervisión continua de las condiciones meteorológicas locales y una respuesta rápida a eventos climáticos.

- Procesamiento y Análisis:

  Los centros de procesamiento de datos de AEMET utilizan redes LAN para el procesamiento y análisis de grandes cantidades de datos meteorológicos. Una LAN eficiente es crucial para realizar cálculos complejos y generar pronósticos precisos.

- Comunicación Interna:

  Los efectivos de AEMET dependen de una red LAN para la comunicación interna, el intercambio de información y la colaboración en tiempo real. Esto incluye el uso de

sistemas de correo electrónico, aplicaciones internas y plataformas de colaboración y puesto de trabajo digital.

- Seguridad de la Red:

  La seguridad de la red LAN es esencial para proteger la integridad de los datos meteorológicos, asegurar la confidencialidad de la información y prevenir accesos no autorizados.

Por otra parte, el Servicio Unificado de Telecomunicaciones de la AGE, tiene como principal pretensión proporcionar a las entidades de la AGE y sus organismos públicos una comunicación de calidad entre todas sus sedes y entre todos sus empleados. Incluye:

- Red corporativa multiservicio y servicio de telefonía fija.
- Comunicaciones móviles
- Internet
- Red internacional

Este servicio consolidado no abarca las necesidades de AEMET en lo que respecta a la gestión de sus propias redes WAN y LAN, aspectos que trascienden los servicios proporcionados por el mencionado servicio unificado. Por ende, AEMET asume directamente la responsabilidad de la administración de estos servicios de redes WAN y LAN, además de las funciones proporcionadas por el Servicio Unificado de Telecomunicaciones de la AGE. Es importante destacar que hay una considerable cantidad de tareas de gestión internas relacionadas con la gestión de la red que no cuentan con el respaldo del servicio unificado de comunicaciones.

Asimismo, el Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS), previsto en la Medida 9 del Plan de Digitalización de las Administraciones Públicas 2021 – 2025, que refuerza a través de servicios horizontales de ciberseguridad las capacidades de prevención, protección, detección y respuesta ante incidentes de ciberseguridad, de forma que gracias a la optimización y las economías de escala se obtenga una mejor eficacia y eficiencia.

Por otra parte, AEMET ha establecido una Oficina Técnica de Seguridad (OTS) como medida estratégica para fortalecer la gestión interna de la seguridad cibernética. La OTS desempeña un papel central en la planificación, implementación y supervisión de las políticas y prácticas de seguridad de la información en toda la organización en coordinación con el COCS. Su misión es garantizar la integridad, confidencialidad y disponibilidad de los activos de información críticos de la AEMET y actuar como punto focal único ante el COCS bajo la supervisión del Responsable de Seguridad de AEMET (RS).

De conformidad con el principio básico de diferenciación de responsabilidades, consagrado en el artículo 11 del RD 311/2021, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, los servicios de gestión de redes WAN y LAN de AEMET excluyen la prestación de servicios propios de la OTS de AEMET, sin perjuicio de la implementación de medidas de seguridad, indicadas por la OTS y de la ineludible colaboración con la OTS bajo la supervisión del Responsable de Seguridad de AEMET.

En el contexto anterior, y debido a la importancia de la explotación, operación y monitorización de las redes WAN y LAN de AEMET, se requiere la contratación de los servicios que implementen servicios de operación, monitorización, explotación de las redes WAN y LAN de AEMET, como activos esenciales que son para la operación y funcionamiento

de AEMET. Además, estos servicios contratados asegurarán la adecuada coordinación con el Servicio Unificado de Telecomunicaciones de la AGE, COCS y OTS de AEMET.

2. OBJETO

Ante la necesidad detectada en el apartado anterior, el objeto del presente pliego es la contratación por la Agencia Estatal de Meteorología (AEMET) de los servicios de gestión y mantenimiento de las redes LAN (redes de área local) de AEMET. Estos servicios podrán desglosarse en:

- Servicios in situ de gestión y mantenimiento de redes LAN (apartado 4.1 y subapartados)
- Servicios no in situ (apartado 4.2 y subapartados)
- Servicio de suministro de pequeño material (apartado 4.3)
- Servicio de control y filtrado de contenidos (apartado 4.4)
- Servicio de gestión del cableado y otros elementos de acceso. Etiquetado y certificación (apartado 4.5)
- Servicio de bolsa de horas (apartado 4.6)
- Servicio de realización de pilotos (apartado 4.7)
- Servicio de transferencia tecnológica (apartado 4.8)

La descripción exhaustiva de estos servicios se desarrolla en los apartados de este PPT indicados anteriormente.

Quedan excluidos del ámbito objetivo de este expediente la prestación de servicios propios de la OTS de AEMET, sin perjuicio de la implementación de medidas de seguridad, indicadas por la OTS y bajo la supervisión del Responsable de Seguridad de AEMET, que sí forma parte de los servicios objeto de este expediente y que serán realizados por parte de los servicios in situ especificados en este expediente.

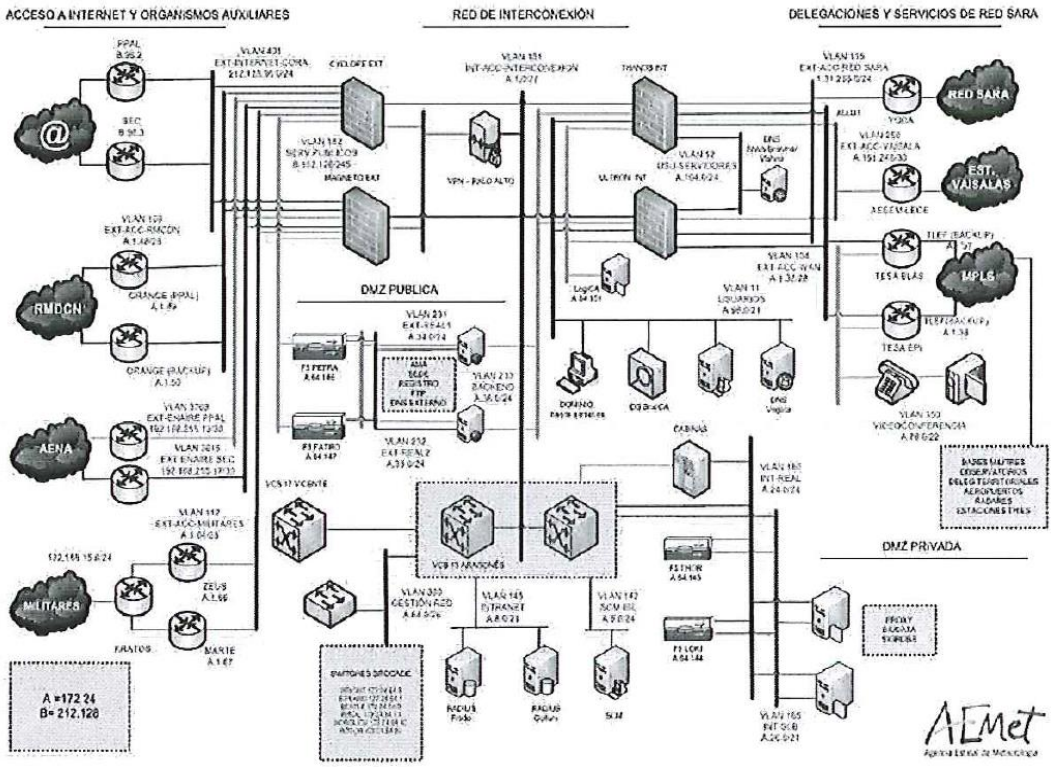
3. DEFINICIÓN DEL ENTORNO TECNOLÓGICO

La definición del entorno tecnológico enumerado en este apartado se realiza, por motivos de seguridad, en términos generalistas. Para mayor nivel de detalle se requiere el acceso a:

- ANEXO I: Sistemas y equipos dentro del objeto del contrato
- ANEXO II: Esquema general de la red de AEMET

3.1 Esquema general de LAN en SSCC

El esquema general de LAN en SSCC de AEMET es el mostrado en la siguiente figura. Para mayor nivel de detalle de la red AEMET, consultar el ANEXO II del presente pliego.



3.2 Descripción general de la red de AEMET

Las líneas principales de los accesos externos en SSCC están diversificados y consolidados en dos equipos enrutadores principales. Telefónica, como operador del Contrato Unificado de la AGE (CORA), dispone dos equipos Juniper en los Servicios Centrales (SSCC) de AEMET. Estos actúan en sus diversos interfaces locales como Equipos de Cliente (EDC) de los servicios proporcionados a AEMET dentro del contrato CORA: Accesos a la WAN de AEMET, a Internet, a la red SARA y los enlaces con ENAIRE.

Las comunicaciones IP/MPLS son transparentes con SSCC, no siendo objeto de este contrato la gestión los routers de IP/MPLS que pertenecen al operador. Los primeros elementos que gestionará el adjudicatario son los conmutadores a los que se conectan estos routers en SSCC y otras sedes.

3.2.1 Servicios WAN en AEMET

Las delegaciones territoriales (DTs), centros meteorológicos (CMs), estaciones meteorológicas aeronáuticas (EMAes), oficinas meteorológicas de defensa (OMDs), los observatorios provinciales (OBs), estaciones de radares, sondeos y estaciones meteorológicas automáticas (EMAs) están conectados por accesos WAN IP/MPLS con la sede de Servicios Centrales. Estos accesos son de distintas configuraciones y capacidades en función de las necesidades de cada tipo de sede, y diferenciando tráfico de datos, VoIP, o videoconferencia.

Con independencia de lo anterior, en los SSCC se dispone además de un acceso WAN diversificado a la red de datos meteorológicos europea (RMDCN). La comunicación con la RMDCN se efectúa a través de 2 líneas (principal y respaldo) gestionadas por operadora

externa. Los routers se gestionan por la propia RMDCN, siendo transparente la comunicación hacia la Red RMDCN. Los enlaces y los equipos de comunicaciones asociados a la RMDCN no son objeto de este contrato, salvo en lo que concierne al soporte al diagnóstico y la coordinación con el operador en caso de incidencias.

3.2.2 Descripción de LAN en SSCC

La infraestructura de red del cliente AEMET está compuesta por una serie de elementos de Nivel 2 y 3, que conforman una topología tipo Campus con sus capas de Distribución y Acceso (No Core).

Si bien los equipos de switching que la conforman poseen capacidades de Datacenter (Brocade VDX), los flujos de tráfico que actúan son Norte-Sur (AEMET-Exterior) y no Este-Oeste (AEMET-AEMET) que es lo habitual en un DataCenter. Dicho flujo de tráfico estaría reflejado a nivel de equipos de SuperComputación que poseen una infraestructura propia, ajena a la que estamos describiendo.

En referencia a las mencionadas capas de Distribución y Acceso, implementadas con dos tipos de hardware distintos para cada una de las capas, se tiene:

Con respecto a la Capa de Distribución se distinguen 4 zonas diferenciadas:

- VCS 13: Proporciona la infraestructura unión con Distribución a la capa de Acceso fundamentalmente. Asimismo aloja otros equipos como acceso a Sedes Remotas, Controladora WIFI, Conexión con RED SARA/MINISTERIO, etc.
- VCS 17: Conforma la capa de Core propiamente dicha. Aquí se alojan sobre todo las infraestucturas de Virtualización y Supercomputación.
- VCS 5: Forma la DMZ y, por tanto, la interconexión entre la doble barrera de Firewalls de AEMET.
- VCS 15: Conforman la infraestructura de switching de equipos externos ajenos al personal de AEMET. En esta zona podemos encontrar servicios tales como los enlaces a la Red CORA/INTERNET, RMDCN y ENAIRE.

Con respecto a la Capa de Acceso, tal y cómo su nombre indica, se refiere a equipos que dotan de servicio a dispositivos de usuario en su mayoría, puntos de acceso para WIFI, etc.

Por otra parte, y con respecto a las plataformas de enrutamiento existen en SSCC:

- Firewalls Externos: donde se realizan los enrutamientos hacia Internet, ENAIRE, red RMDCN, etc.
- Firewalls Internos: cubre los enrutamientos de WIFI's, Administración de Red, Usuarios, Interconexión con Red SARA, etc.
- Niveles 3 en Switches de la Capa de Distribución.

A nivel de enrutamiento, únicamente y por norma general se realiza vía routing estático. Unicamente existe routing dinámico en dos entornos y relacionados con el cliente ENAIRE.

Además de los conmutadores del CPD ya mencionados, existen en SSCC otros grupos de conmutadores (conmutadores de planta) que dan servicio a las distintas plantas del edificio de SSCC conectados por fibra óptica con los equipos de Core.

Dentro de la LAN de SSCC están delimitados los diferentes perímetros y zonas de seguridad mediante un sistema doble de cortafuegos de dos fabricantes diferentes. En este sistema diversificado se ejecutan dos instancias diferentes, actuando una de cortafuegos externo y otra de interno.

Los cortafuegos externos delimitan la zona externa, la DMZ y la conexión a redes internas. Los cortafuegos internos aíslan y controlan el acceso entre las diversas zonas de la Intranet que se pretenden proteger. Estos equipos están instalados siguiendo las recomendaciones del ENS, es decir, actuando en forma de doble barrera.

Tanto en la zona entre los FW externos como en la Intranet, se han creado diversas VLAN en función del servicio que se presta (Gestión, Backup, Usuarios, Servidores). La configuración a nivel 3 de la red se efectúa en los cortafuegos o en los conmutadores centrales multinivel. Estos conmutadores tienen conectados directamente los cortafuegos, servidores situados en el CPD, conmutadores de planta en SSCC y otros equipos de red LAN.

Los servidores que precisan de balanceo se conectan a través de un sistema diversificado de balanceadores, que ejecutan dos instancias virtuales de servicio. El balanceador externo sirve a los sistemas que se destinan a Internet, mientras que el interno atiende los servidores con destino a la Intranet. Con independencia de lo descrito hasta ahora los balanceadores además incorporan la funcionalidad WAF.

Como servidores de túneles VPN se emplean los cortafuegos externos. Además de las conexiones VPN para usuarios y empresas de mantenimiento, existen túneles permanentes con otras empresas y aeropuertos, para distribución de productos de carácter meteorológico.

Por último, en SSCC de AEMET existen un Salón de Actos y diversas Salas de Conferencias utilizadas para reuniones con medios audiovisuales y sistemas de videoconferencia. El mantenimiento de los equipos de videoconferencia y medios audiovisuales no es objeto de este contrato.

3.2.3 Descripción de LAN en DTs, CMs, EMAes y OMDs y otras dependencias

En las DTs, CMs, EMAes, OMDs y sedes de radar están dispuestos uno o varios conmutadores que dan soporte LAN para proporcionar conectividad de datos, VolP, videoconferencia y/o Wi-Fi. La gestión de estos conmutadores, enumerados en el ANEXO I es también objeto de este contrato.

3.3 Planta de equipos objeto del contrato

El equipamiento objeto de contrato y las modalidades de servicio requeridos para cada equipo se describe en el ANEXO I.

4. ALCANCE DE LA CONTRATACIÓN

Los servicios objeto de la contratación serán:

4.1 Servicios in situ de gestión y mantenimiento de redes LAN

Los servicios de gestión de red consisten en las funciones de:

- Monitorización de la red LAN
- Gestión de incidencias
- Implementación de las medidas e iniciativas de seguridad definidas por Oficina Técnica de Seguridad de AEMET

- Gestión de la configuración y administración del conjunto de equipos de infraestructura de red
- Gestión del inventario de equipos y sistemas
- Gestión de garantías y soporte del fabricante
- Gestión del mantenimiento
- Control y filtrado de contenidos
- Gestión del cableado y otros elementos de acceso. Etiquetado y certificación

4.1.1 Monitorización de la red LAN

La función de monitorización de la red LAN (Red de Área Local) de AEMET es esencial para garantizar su rendimiento, seguridad y disponibilidad. Las tareas incluidas en esta función tienen como pretensión garantizar un rendimiento óptimo, la seguridad y la disponibilidad de la red LAN de AEMET, y permitir una respuesta proactiva a posibles problemas. Algunas de las tareas que se incluyen en esta función son:

- Supervisión del tráfico de red:
    - Analizar el tráfico de red para identificar patrones de uso.
    - Detectar y analizar picos de tráfico.
    - Identificar protocolos de red utilizados y aplicaciones que generan tráfico.
- Gestión del ancho de banda:
    - Supervisar el uso del ancho de banda para optimizar su distribución.
    - Identificar y abordar cuellos de botella en la red.
    - Aplicar políticas de calidad de servicio (QoS) según sea necesario.
- Seguridad de la red:
    - Identificar y analizar intentos de intrusiones o actividades maliciosas.
    - Supervisar la seguridad de la red mediante la detección de amenazas y vulnerabilidades.
    - Implementar medidas para proteger contra ataques, como firewalls y sistemas de detección de intrusiones (IDS) etc.
- Disponibilidad y rendimiento:
    - Supervisar el estado y la disponibilidad de los dispositivos de red.
    - Realizar pruebas de rendimiento para evaluar el rendimiento de la red.
    - Identificar y abordar problemas de latencia y pérdida de paquetes.
- Registro y documentación:
    - Mantener registros detallados de eventos de red y cambios en la configuración.
    - Documentar la topología de red, configuraciones y políticas.
    - Facilitar la auditoría y la resolución de problemas mediante registros detallados.
- Gestión de activos de red:
    - Supervisar la conexión y desconexión de dispositivos en la red.
    - Gestionar la asignación de direcciones IP y la resolución de nombres de dominio.
    - Realizar un seguimiento de los cambios en la configuración de dispositivos de red.

- Actualizaciones y parches:
    - Gestionar las actualizaciones de firmware y software de los dispositivos de red.
    - Aplicar parches de seguridad para mitigar vulnerabilidades conocidas.
- Optimización de la red:
    - Identificar oportunidades para optimizar la red y mejorar la eficiencia.
    - Realizar análisis de tendencias para planificar la capacidad de la red.
- Notificación de eventos:
    - Configurar alertas y notificaciones para eventos críticos o anómalos.
    - Establecer umbrales para recibir alertas cuando se superen ciertos límites.
- Formación y documentación:
    - Proporcionar formación y documentación a los usuarios finales y al personal de TI.
    - Mantener al personal actualizado sobre las mejores prácticas de seguridad y uso de la red.

La herramienta de monitorización de nivel 3 estará basada en ZABBIX, puesto que facilita la integración con la monitorización de otros sistemas no objeto de este contrato. Como herramienta de gestión se implementará el Sistema de Gestión del Servicio (SGS) descrito en el apartado 9 de este PPT.

Al finalizar el contrato, cualquier desarrollo, licencia de software o hardware facilitado para esta función quedará en propiedad de AEMET.

Con el fin de proporcionar soluciones técnicas eficientes en los plazos adecuados a las incidencias y necesidades que surjan durante el contrato, el personal del adjudicatario deberá actuar, cuando así se solicite, como representante e interlocutor técnico por parte de AEMET ante los fabricantes o suministradores de equipamiento, operadores y otros prestadores de servicios, usuarios internos o externos y demás agentes a los que las redes LAN o WAN de AEMET proporcionen conectividad y servicios.

4.1.2 Gestión de incidencias

AEMET requiere funciones de gestión de incidencias en la red de comunicaciones, como parte crítica de la administración de una red que se enfoca en identificar, informar, seguir y resolver problemas y anomalías que puedan surgir en su infraestructura de comunicaciones. El objetivo principal es mantener el rendimiento, la disponibilidad y la integridad de la red. Se requiere cubrir los siguientes componentes del servicio:

- Detección de incidencias: deberá cubrirse la detección de problemas o anomalías en la red. Estos problemas pueden incluir caídas de conexiones, latencia excesiva, pérdida de paquetes de datos, violaciones de seguridad, entre otros.
- Registro de incidencias: una vez que se detecta una incidencia, se registrará en el sistema acordado con la Dirección Técnica de la AEMET. Esto incluye la recopilación de información relevante sobre el problema, como la ubicación, la hora de inicio, la severidad, las descripciones detalladas y la causa probable.
- Clasificación y priorización: para la óptima resolución de las incidencias, éstas se deberán clasificar y priorizar en función de su gravedad y el impacto en las operaciones de la red.

- Asignación de recursos: una vez que se ha clasificado una incidencia, el coordinador técnico asignado por la adjudicataria deberá asignar los recursos adecuados para su resolución. Esto deberá incluir a los técnicos de red, ingenieros de seguridad y/o personal de soporte que la adjudicataria haya asignado a la prestación de sus servicios.
- Resolución de incidencias: los técnicos deberán aplicar los procedimientos aprobados por la Dirección Técnica para resolver cada incidencia. Se incluye la intervención en cambios en la configuración de la red, actualizaciones de firmware, solución de problemas o medidas de seguridad adicionales.
- Comunicación con los interesados: durante todo el proceso, es importante mantener a los interesados informados sobre el estado de la incidencia. Los técnicos deberán asumir las notificaciones correspondientes para cada ticket generado.
- Seguimiento y documentación: cada incidencia deberá documentarse cuidadosamente, incluyendo detalles sobre las acciones tomadas, el tiempo requerido para la resolución y cualquier lección aprendida. Se utilizará esta documentación para el análisis posterior y para la mejora continua de la red.
- Análisis de tendencias: los técnicos deberán valorar las posibles tendencias y patrones de problemas recurrentes, en orden de identificar posibles problemas subyacentes en la red, para prevenir futuras incidencias similares.
- Informes y métricas: Los servicios de gestión de incidencias a menudo generan informes periódicos que proporcionan una visión general del rendimiento y la eficacia de la gestión de incidencias en la red.

Este servicio de gestión de incidencias en la red de comunicaciones pretende minimizar el tiempo de inactividad, mantener la satisfacción del usuario y proteger la seguridad de la red al abordar de manera rápida y efectiva cualquier problema que pueda surgir. La aplicación de este servicio deberá cubrir:

- La colaboración en la implementación de medidas sobre la infraestructura de red definidas por la Oficina Técnica de Seguridad de AEMET en la resolución de incidencias de Seguridad, o bien, indicadas por la Oficina Técnica de Seguridad de AEMET a instancias del COCS.
- La colaboración en la implementación de medidas sobre la infraestructura de red indicadas por la Oficina Técnica de Seguridad de AEMET a instancias del COCS en la resolución de incidencias de Seguridad.
- Las incidencias originadas en los equipos, sistemas y redes LAN que son responsabilidad directa del adjudicatario (Anexo I).
- Las incidencias originadas en equipos y redes WAN a las que está conectado AEMET, en las que el adjudicatario actuará como representante de AEMET ante los operadores y otros organismos implicados.

4.1.3 Implementación de las medidas e iniciativas de seguridad definidas por Oficina Técnica de Seguridad de AEMET

La empresa adjudicataria deberá seguir las indicaciones del personal de la OTS de AEMET, bajo la supervisión del Responsable de Seguridad de AEMET, de modo que se logre reducir el riesgo a un nivel controlable. Se incluyen las siguientes tareas de orden principal:

- Asignación de recursos: se deberá incluir a los técnicos de red, ingenieros de seguridad y/o personal de soporte que la adjudicataria haya asignado a la prestación de sus servicios.
- Implementación: los técnicos deberán aplicar los procedimientos aprobados por la OTS, bajo la supervisión del Responsable de Seguridad de AEMET, para aplicar las medidas de protección. Se incluye la intervención en cambios en la configuración de la red, actualizaciones de firmware, solución de problemas o medidas de seguridad

adicionales. Asimismo, se implementan medidas de seguridad para proteger la red contra amenazas y vulnerabilidades. Esto incluye la configuración de cortafuegos, sistemas de detección de intrusiones y políticas de seguridad.

- Seguimiento y documentación: cada implementación deberá documentarse cuidadosamente, incluyendo detalles sobre las acciones tomadas, el tiempo requerido para la resolución y cualquier lección aprendida. Esta documentación estará a disposicion de la OTS y del Responsable de Seguridad de AEMET en cuaquier momento.

4.1.4 Gestión de la configuración y administración del conjunto de equipos de infraestructura de red

La adjudicataria deberá asumir la configuración de equipos de red de comunicaciones, establecidos en el Anexo I, como un conjunto de actividades y procesos diseñados para asegurar que los dispositivos de red -enrutadores, conmutadores, cortafuegos y otros componentes de infraestructura de red- estén configurados y optimizados para funcionar de manera eficiente, segura y de acuerdo con los requisitos específicos de AEMET. Quedarán incluidas las siguientes actividades de orden principal:

- **Planificación inicial**: a partir de la definición de requisitos de la red se establecerán objetivos específicos. Esto incluye la identificación de los dispositivos necesarios, el análisis de variación de la topología de la red y los protocolos de comunicación que se utilizarán.
- **Selección de equipos**: los técnicos deberán seleccionar los dispositivos de red adecuados, entre los existentes en la infraestructura, en función de las necesidades para la modificación de las configuraciones.
- **Instalación física**: los técnicos deberán verificar que los equipos estén conectados de manera adecuada y segura.
- **Configuración de dispositivos**: será objeto del servicio la programación de los dispositivos para que funcionen según las especificaciones de la red, incluyendo la configuración de direcciones IP, enrutamiento, políticas de seguridad, reglas de firewall y otros parámetros.
- **Optimización del rendimiento**: de manera sistemática, se deberán realizar ajustes para optimizar el rendimiento de la red, como la asignación de ancho de banda, la gestión de la calidad del servicio (QoS) y la resolución de problemas de congestión.
- **Actualizaciones y parches**: se deberá aplicar un procedimiento para el seguimiento de actualizaciones de firmware y parches de seguridad, para mantener los dispositivos de red actualizados y protegidos contra amenazas conocidas.
- **Integración con otros sistemas**: el servicio deberá prestar colaboración con los responsables de otros servicios que se integran con los de la red, como son los de sistemas de gestión de identidad, sistemas de gestión de proyectos y sistemas de almacenamiento, para garantizar la interoperabilidad y la eficiencia.
- **Documentación y registro**: se deberá mantener la configuración de red, incluyendo sus diagramas de topología, las listas de configuración y los registros de cambios, para facilitar la resolución de problemas y el mantenimiento continuo.
- **Formación del personal**: los técnicos deberán encargarse de trasladar conocimiento al personal de TI y/o a los usuarios finales para asegurarse de que comprendan cómo interactuar con la red de manera segura y eficiente, conforme a las nuevas configuraciones que así lo requieran.

La aplicación de este servicio deberá cubrir la administración, el control de cambios y la documentación de equipos y sistemas establecidos en Anexo I.

4.1.5 Gestión de inventario de equipos y sistemas

La gestión de inventario de equipos y sistemas es crucial para garantizar el buen funcionamiento de los servicios de red de AEMET, ya que ayuda a optimizar los recursos, reducir costos y mejorar la eficiencia operativa. Entre las tareas que deberá realizar la empresa relacionadas con la gestión de inventario de equipos y sistemas y dentro del ámbito objetivo de este expediente residen:

- Inventario Inicial:

  Realización de un inventario inicial detallado de todos los equipos y sistemas dentro del ámbito objetivo de este expediente. Deberá incluir información como número de serie, modelo, fecha de adquisición, valor, ubicación física y estado.

- Categorización:

  La empresa adjudicataria clasificará los equipos y sistemas en categorías para facilitar la gestión. Los criterios de categorización podrán ser por función, departamento, ubicación, etc. Estos serán determinados por AEMET.

- Registro de Movimientos:

  La empresa adjudicataria registrará todos los movimientos de equipos, ya sea traslados entre departamentos, reparaciones, mantenimientos, o desincorporaciones.

- Actualización Regular:

  Mantendrá actualizado el inventario de forma regular. A medida que se realicen cambios en el estado de los equipos, actualiza la información en el sistema.

- Auditorías Periódicas:

  Se realizarán auditorías periódicas para verificar la precisión del inventario físico con respecto a los registros en el sistema. Se realizarán al menos una auditoría de inventario de equipos y sistemas.

- Seguridad:

  Se implementarán medidas de seguridad para proteger los equipos valiosos determinadas por la Oficina Técnica de Seguridad de AEMET bajo la supervisión del Responsable de Seguridad.

- Gestión de Ciclo de Vida:

  La empresa licitadora planificará y gestionará el ciclo de vida de los equipos. Esto implicará considerar la obsolescencia, renovaciones, actualizaciones y la disposición adecuada al final de la vida útil.

- Automatización:

  La empresa licitadora, donde sea posible, utilizará la automatización para simplificar procesos repetitivos, como la generación de informes o las actualizaciones de inventario.

- Formación del Personal:

La empresa adjudicataria proporcionará formación al personal sobre cómo utilizar el sistema de gestión de inventario y la importancia de mantener la precisión en los registros.

- Respaldo y recuperación:

  La adjudicataria deberá garantizar que se implementen estrategias de respaldo y recuperación de la documentación.

En definitiva, la adjudicataria:

- El adjudicatario será responsable de la adecuada gestión de la documentación correspondiente al equipamiento físico y lógico objeto de este contrato.
- Mantendrá informado a AEMET con la suficiente antelación del estado de actualización de los equipos activos.
- Mantendrá informado a AEMET de la necesidad de renovación o sustitución de los mismos por causas técnicas o comerciales, del vencimiento de plazos de licencias, garantías o soportes de los fabricantes y de las posibles soluciones o alternativas tecnológicas que se puedan adoptar para afrontar estas circunstancias.
- Se responsabilizará de la gestión de la información de licencias y servicios de soporte TIC contratados en AEMET y que este les facilitará, en el ámbito de redes y seguridad (como fechas de vencimiento y prórrogas).

4.1.6 Gestión de garantías y soporte del fabricante

La adjudicataria deberá asumir el proceso de gestionar reclamaciones y resolver problemas relacionados con la garantía, frente al proveedor de AEMET, en nombre de esta. Este servicio es fundamental para asegurar que los equipos de red sean reparados o reemplazados de manera oportuna y eficiente si experimentan fallos cubiertos por la garantía. Quedarán incluidas las siguientes actividades de orden principal:

- **Recepción y evaluación de reclamaciones**: cuando se experimente un problema con un equipo de la red de comunicaciones de AEMET, que esté dentro del período de garantía, se evaluará la validez de una posible reclamación, verificando si el problema está cubierto por la garantía del fabricante.
- **Coordinación con el fabricante**: una vez que la adjudicataria haya determinado que el problema está cubierto por la garantía, los técnicos deberán ponerse en contacto con el fabricante del equipo de red. Esto puede incluir la creación de un expediente de garantía, la recopilación de información sobre el equipo y el registro de la reclamación en el sistema del fabricante.
- **Seguimiento y gestión de la garantía**: la adjudicataria deberá seguir de cerca el proceso de garantía, asegurándose de que el fabricante cumpla con los plazos y procedimientos especificados en el acuerdo de garantía. Esto incluye el envío del equipo defectuoso al fabricante si es necesario.
- **Comunicación constante**: la adjudicataria deberá mantener informada a AEMET para proporcionar actualizaciones sobre el estado de la garantía y el progreso de la resolución de las incidencias en garantía. Deberá actuar como punto de contacto entre AEMET y sus proveedores para responder a preguntas y preocupaciones.
- **Resolución de problemas**: si surgen problemas en el proceso de garantía, como retrasos o disputas con el fabricante, la adjudicataria deberá trabajar para resolverlos de manera eficaz, lo que puede incluir la mediación entre ambas partes.
- **Reemplazo o reparación de equipos**: cuando se apruebe la aplicación de garantía, la adjudicataria deberá asegurarse de que AEMET reciba un equipo de reemplazo o que el equipo defectuoso sea reparado según lo acordado por el fabricante.

- **Registro y documentación**: deberá mantenerse un registro completo de todas las comunicaciones y transacciones relacionadas con la garantía, incluyendo detalles sobre los equipos afectados, fechas de reclamaciones, resoluciones y acuerdos.
- **Informe y análisis**: la adjudicataria deberá proporcionar informes periódicos a AEMET sobre el rendimiento y la eficiencia del proceso de garantía, para identificar posibles oportunidades de mejora.

En los casos en que los equipos gestionados estén en garantía, el adjudicatario asumirá la gestión de la misma y de los servicios de soporte asociados. Para ello contactará con los servicios técnicos del responsable de la garantía, con quien concertará la operativa de acceso a su servicio y los informes de control y seguimiento.

Los niveles de servicio de los acuerdos con los fabricantes, para todos los equipos de criticidad máxima (apartado 4.1.7.1 de este PPT y ANEXO I) será de 7x24x365.

4.1.7 Gestión del mantenimiento

AEMET requiere la realización de las funciones de mantenimiento de su red interna de comunicaciones como un conjunto de actividades planificadas y proactivas destinadas a garantizar el funcionamiento óptimo, la disponibilidad continua y la protección de sus sistemas de comunicaciones. Estos servicios son esenciales para garantizar que la red siga siendo eficiente, confiable y cumpla con los requisitos operativos que tiene asignados. El servicio deberá contemplar los diferentes aspectos que se enumeran:

- Monitorización continua: mediante una supervisión constante de la red para identificar problemas potenciales, identificar cuellos de botella, evaluar el rendimiento y detectar cualquier anomalía.
- Mantenimiento preventivo: se incluyen las tareas programadas y rutinarias para prevenir problemas antes de que ocurran. Esto puede incluir actualizaciones de firmware, parches de seguridad, optimización de configuraciones y revisión de políticas de seguridad.
- Resolución de problemas: para abordar problemas inesperados en tiempo real. Esto puede incluir la solución de problemas de conectividad, la restauración de servicios interrumpidos y la identificación de causas fundamentales de problemas.
- Actualizaciones y parches: aplicando actualizaciones de software y parches de seguridad para mantener la red protegida contra vulnerabilidades conocidas y para asegurarse de que funcione con las últimas características y mejoras. Esta operativa deberá garantizar la aplicación de estas actualizaciones en un plazo no superior a tres meses desde la publicación por parte del fabricante.
- Gestión de activos: con el propósito de anticiparse a la planificación de reemplazos y actualizaciones, deberá realizarse un seguimiento de todos los componentes de la red, como servidores, enrutadores, conmutadores, firewalls internos y otros dispositivos.
- Optimización de la red: deberá efectuarse un análisis sistemático del rendimiento de la red, para proporcionar recomendaciones que mejoren la eficiencia y la capacidad de la red, así como la redistribución del tráfico y la actualización de hardware obsoleto.
- Copias de seguridad y recuperación de desastres: encargándose de la aplicación de procedimientos de copia de seguridad y recuperación para proteger los datos críticos en caso de fallos de hardware o desastres naturales.
- Seguridad: encargándose de implementar y mantener políticas de seguridad de la red, en los cortafuegos existentes, los sistemas de detección de intrusiones, los mecanismos de autenticación y cifrado, con el propósito de proteger la integridad y confidencialidad de la red.
- Cumplimiento normativo: el servicio deberá garantizar que la red cumpla con los requisitos legales y reguladores aplicables, manteniendo la documentación de auditoría y los registros para demostrar el cumplimiento.

- Documentación de la red: el servicio deberá incluir la actualización de la documentación de configuración de la red, sus esquemas de topología, la definición de procedimientos de mantenimiento y otros aspectos relacionados con la red para facilitar la resolución de problemas y las futuras expansiones.

Este mantenimiento de la red de comunicaciones se circunscribe a los activos especificados en el Anexo I, sobre los que se deberá garantizar un funcionamiento ininterrumpido de la red, maximizar la inversión en infraestructura de red y proteger la seguridad de los datos y la información que fluyen a través de ella. La adjudicataria deberá marcarse los objetivos de minimizar el tiempo de inactividad de los sistemas, mantener la productividad de la red, y que los activos estén preparados para las demandas cambiantes de las comunicaciones durante la evolución de los servicios que soportan de AEMET.

4.1.7.1 Niveles de criticidad

- Se definen los siguientes como **"Equipos de máxima criticidad":** conmutadores instalados en SSCC en el CPD (Core) y CNP, balanceadores de aplicaciones, cortafuegos, servidores de túneles, servicios DNS/DHCP, sistemas NAC y RADIUS.

- Se definen los siguientes como **"Equipos de criticidad media":** Resto de conmutadores de SSCC en Madrid y conmutadores de DTs y OMAs.

4.1.8 Control y filtrado de contenidos

Los licitadores deberán incorporar en su propuesta de servicios, la prestación de un servicio de filtrado de contenidos, deslocalizado, para la protección de los terminales de trabajo de los empleados de AEMET. Este servicio deberá cubrir un mínimo de 1.300 terminales de trabajo durante la vida del contrato.

Tras la pandemia, el teletrabajo sigue presentando una importancia estratégica para los organismos y empresas, entre ellos AEMET, teniendo muchas de ellas planes para profundizar en el acceso de los trabajadores remotos o itinerantes a los diferentes recursos corporativos (terminales remotos, impresoras…). Desde AEMET, este acceso se debe hacer de forma segura, pero tiene que ser lo más fácil y eficiente posible para los usuarios en remoto. Por este motivo, es fundamental que se implemente sobre las plataformas ya desplegadas en la infraestructura de comunicaciones y seguridad, FortiGate y FortiAuthenticator ya desplegados en AEMET.

Para implantar este servicio, el primer requerimiento es la adquisición de un **Agente VPN** con funcionalidades de seguridad para establecer una comunicación con el equipo FortiGate, detrás del cual se encuentran los recursos corporativos, y el segundo requerimiento es el suministro de la **herramienta de gestión FortiClient EMS**. De esta forma, EMS podrá alimentar a los FortiClient firewall internos con la información necesaria para realizar la conexión con el recurso corporativo, a la vez que informará a los equipos NGFW FortiGate desplegados en AEMET de si determinados equipos tienen o no permiso para acceder a esos recursos.

En una red critica como la de AEMET, es requisito fundamental implementar un servicio de control y filtrado de contenidos ZTNA. Una de las funcionalidades imprescindibles a usar dentro del concepto Zero Trust en entornos con políticas de firewall y VPN, es el uso de los tags compartidos desde la consola EMS al NGFW dentro de las políticas. De esta forma, se podrá disponer de una granularidad muy elevada en los accesos controlados por el firewall. Para ello, se requiere del agente nativo ZTNA de la solución (nativo en la solución FortiClient) que en conjunto con los NGFW y el Authenticator para la identidad del usuario, ya desplegados en la red de AEMET, proporcionan la postura del dispositivo y Single Sign-On, SSO, necesarios. La postura del dispositivo se refiere a la evaluación del estado de

seguridad y cumplimiento de políticas de un dispositivo antes de permitir su acceso a la red. Esta evaluación se realiza para asegurarse de que el dispositivo cumple con ciertos estándares de seguridad y configuraciones antes de ser admitido en la red.

Las características del servicio deberán satisfacer, como mínimo, los siguientes requisitos:

- El servicio se encargará de supervisar todas las actividades del navegador web para aplicar la política corporativa de uso aceptable y granular de su seguridad web, filtrado de contenido web y control granular de software como servicio (SaaS), apoyándose en, al menos, 75 categorías diferentes.
- El servicio deberá contar con la capacidad de configurar listas negras y blancas, así como políticas dentro y fuera de la red e importar políticas de Web Filtering desde los firewalls existentes, para una aplicación consistente de las políticas corporativas de navegación web.
- Se requiere la capacidad de integración con la funcionalidad de SafeSearch de Google, para aprovechar este mecanismo externo de protección.
- El servicio deberá ser capaz de la inspección del tráfico cifrado HTTPS a través de conectores en los navegadores de la estación de trabajo (al menos, Chrome, Firefox y Microsoft Edge) sin necesidad de aplicar intercepción SSL, de manera que este cifrado no evada la aplicación de las políticas corporativas.
- Posibilidad de bloquear, permitir, advertir y monitorizar el tráfico web basado en la categoría URL o filtros URL personalizados.
- Posibilidad de crear listas de exclusión de filtros de URL personalizados, que anulen categorías por defecto del servicio.
- Compatibilidad con sistemas operativos de escritorio Microsoft Windows y Apple Mac.
- Seguimiento de la disponibilidad de la protección de punto final a través de mecanismos de telemetría.
- El servicio deberá proporcionar un mecanismo de integración del filtrado de URLs para cada uno de los terminales de trabajo, sobre los firewalls existentes en AEMET, de manera que se consiga la cooperación en la protección de los terminales de trabajo a través de una amplia visibilidad de los mismos en los firewalls de AEMET, de manera que se consiga el control de cumplimiento de las políticas corporativas, la administración de vulnerabilidades, incluyendo la presencia de software malicioso y/o que entrañe algún riesgo en los equipos.
- El servicio de filtrado web requerido deberá prestarse cuando los usuarios se encuentran dentro de la red corporativa protegidos por los firewalls existentes, pero también cuando los usuarios salen de la red mediante la generación de perfiles de protección off-net.
- La adjudicataria deberá gestionar las políticas oportunas sobre los firewalls existentes en AEMET, para denegar el acceso a los puntos finales con vulnerabilidades conocidas o poner en cuarentena los puntos finales comprometidos.
- La adjudicataria deberá actualizar las listas y los parámetros del sistema de filtrado, diariamente en los servidores de AEMET.
- El servicio deberá incluir la aplicación de la política de seguridad corporativa y los criterios de uso, como la severidad de las vulnerabilidades no parcheadas, el software en ejecución, el Web Filtering y la postura de seguridad.
- Permitirá aplicar las políticas tanto a los trabajadores remotos como a los que se encuentran en la red internaen el campus.
- Permitirá acceder a una aplicación específica solamente para esa sesión.
- Verificará la identidad del usuario, la identidad del dispositivo, la actitud del dispositivo antes de conceder acceso.
- El servicio proporcionará VPN, escaneo de vulnerabilidades, filtrado de URL y protección de endpoint con un solo agente.
- Establecerá el cifrado TLS automáticamente entre el endpoint y el proxy de acceso, ocultando el tráfico.
- El servicio por tanto, deberá ser capaz de aplicarse a cualquier dispositivo que accede a la red. De manera que, deba ser autenticado, además de comprobar el

estado de salud del equipo desde el que realiza la conexión. Ese chequeo será continuo mientras esté conectado a la red corporativa.

Se requiere, por tanto, de una infraestructura compatible con la plataforma hardware que actualmente tiene la AEMET, con las siguientes características técnicas:

- Garantizará un acceso remoto seguro con funcionamiento continuo, SSL/Ipsec VPN que respalda la segmentación de la red, admisión condicional e integración con plataformas de inicio de sesión único y autenticación de múltiples factores.
- Dispondrá de seguridad de confianza cero: para que un trabajador remoto se conecte a la red con un mínimo nivel de control. Esta edición habilitará túneles cifrados, al igual que filtrado de URL y control de dispositivos USB. Se incluirá la gestión central a través de la plataforma EMS.
- Deberá tener administración central a través de EMS:
  - Implementación y aprovisionamiento centralizado: Permitirá a los administradores implementar software de punto final de forma remota y realizar actualizaciones controladas. Hará que la implementación de la configuración del cliente en múltiples endpoints sea una tarea fácil con solo un clic en un botón.
- Panel de Vulnerabilidad: Ayudará a gestionar la superficie de ataque de una organización. Todos los puntos finales vulnerables se identificarán fácilmente para una acción administrativa.
- Integración de Windows AD: Ayudará a sincronizar la estructura AD de una organización en EMS para que las mismas unidades de organización (OU) puedan usarse para la administración de endpoints. El estado de los endpoints en tiempo real proporcionará siempre información actualizada sobre la actividad de los endpoints y los eventos de seguridad.
- Registro de generación de informes central:
  - Simplificará la elaboración de informes de cumplimiento y el análisis de seguridad mediante cualquier producto SIEM.
- Conector dinámico Security Fabric:
  - EMS creará grupos virtuales basados en postura de seguridad del endpoint. Estos grupos virtuales serán recuperados por los dispositivos de seguridad y utilizados en la política firewall para el control del acceso dinámico. Los grupos dinámicos ayudarán a automatizar y simplificar el cumplimiento de las políticas de seguridad.
- Agente de vulnerabilidad y corrección:
  - Asegurará la higiene de los endpoints y los fortalecerá para reducir la superficie de ataque. Identificará los endpoints vulnerables y priorizará las vulnerabilidades del software y del sistema operativo no parcheadas con opciones de parches flexibles que incluirán parches automáticos.
- SSL (Secure Socket Layer) VPN (Virtual Private Network) con MFA:
  - Permitirá un túnel cifrado fácil de usar que atravesará casi cualquier infraestructura
- Ipsec VPN con MFA:
  - Permitirá un túnel cifrado fácil de usar proporcionando mayor capacidad de proceso VPN
- Control de dispositivos USB:
  - Evitará que dispositivos USB no autorizados accedan al host
- Túnel dividido:
  - Proporcionará respaldado por túneles Zero Trust y VPN, el túnel dividido permitirá una experiencia de usuario optimizada
- Inventario Software:
  - Proporcionará visibilidad en aplicaciones de software instaladas y gestión de licencias que mejorará la higiene de seguridad. Podrá

utilizar la información de inventario para detectar y eliminar aplicaciones innecesarias u obsoletas.

- Etiquetado Interno
  - El etiquetado, se utilizará para la segmentación de la red interna

Los usuarios y sus grupos de pertenencia, que implican los permisos de navegación, se obtienen del LDAP institucional (Open LDAP).

4.1.9 Gestión del cableado y otros elementos de acceso. Etiquetado y certificación

Se requieren capacidades de gestión de cableado de la red de comunicaciones de AEMET que cubra un conjunto de actividades y prácticas destinadas a planificar, diseñar, instalar, organizar y mantener eficazmente la infraestructura física de cables en la red de comunicaciones. Este servicio es esencial para garantizar que los cables, conectores y componentes de la red estén instalados y mantenidos de manera que la red funcione de manera confiable, eficiente y cumpla con los estándares de rendimiento. La especificación del servicio es:

- Peinado 3 armarios/año
- Reubicación 5 equipos
- Auditoría de cableado
- 50 nuevas tomas/año

El servicio deberá contemplar los diferentes aspectos que se enumeran:

- Planificación inicial: cada intervención deberá contemplar una fase de planificación en la que se definan los requisitos de cableado de la red, incluyendo determinar la topología de la red, la capacidad requerida, las ubicaciones de los dispositivos de red y las necesidades de futuro crecimiento. Adicionalmente, se realizará una auditoría inicial del estado del cableado tomada a través de un muestreo significativo de los puntos de acceso ubicados en todas las plantas del edificio de Servicios Centrales de AEMET y a través del cual se emitirá un informe de actuaciones a tener en cuenta según el nivel de criticidad.
- Diseño de la infraestructura de cableado: la adjudicataria deberá crear un diseño detallado por cada intervención, que especifique la disposición de los cables, la ubicación de los puntos de acceso, las rutas de cableado, las normas y estándares a seguir, y la elección de los tipos de cables y conectores adecuados.
- Instalación de cables: incluyendo la instalación física de cables de acuerdo con el diseño, asegurándose de que los cables estén correctamente tendidos, etiquetados y protegidos para garantizar un rendimiento óptimo y minimizar interferencias.
  - Se incluyen los puntos de acceso (rosetas) y el peinado de armarios de distribución en el cableado estructurado de la red corporativa de AEMET.
- Conexión de dispositivos de red: para la conexión de los dispositivos de red, como conmutadores, enrutadores, servidores y puntos de acceso, a la infraestructura de cableado.
- Organización y etiquetado: cada intervención incluirá las labores de etiquetado y organización de los cables de manera que sea fácil identificar la función y la ubicación de cada uno. Adicionalmente, la adjudicataria ejecutará el etiquetado del cableado existente en el CPD y que enlaza con los switches de agregación de planta. Esta auditoría inicial no incluirá los switches de acceso de usuarios.
- Gestión de puntos de acceso: se instalarán y gestionarán las tomas de red en las ubicaciones apropiadas, como puntos de acceso a la red, para permitir la conexión de dispositivos finales.
- Pruebas y certificación: cada intervención incluirá las pruebas exhaustivas para garantizar que los cables funcionen correctamente y cumplan con las normas y

estándares de rendimiento (pruebas de continuidad, pruebas de velocidad de transmisión y otras pruebas de calidad)

- Adicionalmente, se pide que la adjudicataria realice la certificación del cableado de la sede central de la AEMET. La certificación de la instalación deberá incluir la realización de las mediciones de certificación y la realización de la documentación, incluyendo la determinación de la causa de los fallos detectados y el planteamiento de la solución a dichos problemas.
- Documentación y registro: cada intervención deberá incluir la documentación detallada que incluya los planos de cableado, registros de pruebas, listas de inventario y otros datos pertinentes.
- Mantenimiento y gestión del cambio: a medida que la red evolucione, podrán solicitarse modificaciones, expansiones o actualizaciones en el cableado, y que estas se gestionen de manera eficiente y documentada.
- Respaldo y recuperación: la adjudicataria deberá establecer prácticas de respaldo para asegurarse de que la documentación y la configuración del cableado estén respaldadas y se puedan recuperar en caso de desastres.
- La adjudicataria se encargará de ejecutar las tareas necesarias para documentar, etiquetar e inventariar todo el tendido de cableado de troncales entre switches de Core del CPD y switches de planta en la sede de SSCC.

El oferente suministrará a AEMET una herramienta de gestión del cableado que permita implementar los anteriores requerimientos de este servicio.

4.2 Servicios no in situ

Los servicios no in situ consiste en las funciones de:

4.2.1 Función de monitorización remota

Se requieren capacidades de monitorización de la red de comunicaciones para garantizar el rendimiento, la disponibilidad y la seguridad de una red de comunicaciones. Este servicio implica la supervisión constante de la red para recopilar información valiosa sobre su estado y funcionamiento. Esta función deberá contemplar los diferentes aspectos que se enumeran:

- Recopilación de datos: el servicio deberá recopilar datos de toda la red de gestión fuera de banda, que pueden incluir información sobre el volumen de datos, la latencia, la utilización de ancho de banda, los errores de transmisión, los eventos de seguridad, la conectividad de dispositivos, etc.
- Supervisión en tiempo real: se deberá realizar una monitorización en tiempo real para que los administradores de la red pueden detectar problemas y tomar medidas inmediatas para abordarlos.
- Alertas y notificaciones: se requiere una oportuna configuración para generar alertas y notificaciones cuando se detectan problemas o se superen umbrales predefinidos. Estas alertas deberán poder enviarse por correo electrónico, o como notificaciones en una consola de administración.
- Generación de informes: deberán emitirse informes mensuales, como mínimo, para comprender mejor el rendimiento de la red a lo largo del tiempo y como herramienta de asistencia a la toma de decisiones. Estos informes deberán incluir datos históricos, tendencias y métricas clave.
- Análisis de tráfico: la adjudicataria deberá suministrar una herramienta, licenciada durante toda la duración del contrato, para la identificación de patrones de uso de la red, acerca de qué aplicaciones consumen más ancho de banda y qué dispositivos son los más activos. En particular, el servicio de monitorización deberá garantizarse la disponibilidad de métricas con las siguientes características:

- Recopilación y presentación de informes para Cisco CBQoS (Calidad de servicio basada en clases) y NBAR (Reconocimiento de aplicaciones basado en red)
- Compatibilidad con los protocolos NetFlow y NSEL de Cisco, QUIC, J-Flow de Juniper Networks, además de sFlow e IPFIX.
- Control y establecimiento de alertas basadas en umbrales sobre el tráfico de red y el uso del ancho de banda. En particular:
  - Cuando remitentes o receptores sobrepasan los umbrales de ancho de banda.
  - Cuando el tráfico de la interfaz sobrepasa los umbrales de utilización.
  - Cuando se sobrepasan las conexiones fallidas y la cantidad de umbrales de socios de conversación.
- Detalle de información de tráfico de red acerca de:
  - Remitentes, receptores y conversaciones.
  - Dominios del remitente y del receptor.
  - Países del remitente y del receptor.
  - Aplicaciones y protocolos.
  - Tráfico entrante y saliente de la interfaz.
  - Utilización entrante y saliente de la interfaz.
  - Uso de ancho de banda por parte de hosts y grupos.
  - Conexiones sospechosas y puertos Tor.
- El licenciamiento mínimo deberá incluir la funcionalidad de gestión sobre 300 dispositivos durante la vida del contrato.
- La funcionalidad de análisis no deberá tener limitación de dispositivos durante la vida del contrato.

- Diagnóstico de problemas: la adjudicataria deberá suministrar una herramienta (**herramienta de análisis de tráfico**), licenciada durante toda la duración del contrato, de diagnóstico que permita a los administradores de red identificar y resolver los problemas de manera eficiente. La utilidad que aproveche el servicio deberá garantizar el cumplimiento de los siguientes requisitos:
  - Cumplimiento del estándar ISO/IEC 18598.
  - Disponibilidad en tiempo real de control sobre todas las conexiones en la sala de telecomunicaciones.
  - Monitorización de cada puerto de conexión para registrar y verificar continuamente los cambios en una base de datos central.
  - Disponibilidad de los informes en castellano.
  - Disponibilidad del detalle de servicios suministrados en cada puesto de trabajo.
  - Permitirá la gestión electrónica de las órdenes de trabajo para comprobar la correcta realización de estas.
  - Deberá estar disponible en entorno Web para su potencial utilización por parte de los técnicos desplazados in situ.
  - Deberá ser compatible con Simple Network Management Protocol (SNMP) y soportará las versiones SNMPv1, SNMPv2c y SNMPv3.
  - Deberá soportar comunicaciones IPv6.
  - Con capacidad de importar, mostrar e imprimir planos CAD para una representación precisa de los planos de planta.
  - Deberá permitir arrastrar y soltar para poblar los planos de planta con los objetos de la base de datos.
  - Los objetos de la base de datos que se coloquen en un plano de planta deben ser completamente funcionales para que las capacidades de administración del sistema puedan administrarse directamente desde el plano de planta.
  - Proporcionará capacidades para documentar la infraestructura de cableado de planta externa que incluye mapas del campus, bóvedas de cableado, conductos, cajas de empalme, etc.
  - Deberá tener capacidad de descubrir automáticamente el hardware inteligente instalado (paneles/bandejas de parcheo inteligentes y equipos de gestión

inteligente) en cada rack y completar automáticamente esta información en su base de datos.
    - Deberá tener capacidad de descubrir automáticamente la configuración de los switches administrados (entorno LAN y SAN) y luego registrar automáticamente esa información en su base de datos.
    - Deberá tener capacidad de descubrir automáticamente los dispositivos en red que están conectados a los switches de red administrados (entornos LAN y SAN) y registrar esa información en su base de datos.
    - Deberá tener capacidad de descubrir automáticamente la dirección IP, la dirección MAC, el WWN y la información de Host Name para los dispositivos de red y luego registrar automáticamente esa información en su base de datos.
    - Deberá tener capacidad de detectar cuándo un dispositivo de red se ha movido o cambiado su ubicación física.
    - Deberá tener capacidad de enviar correos electrónicos a un personal específico, ejecutar aplicaciones o enviar traps SNMP en tiempo real sobre eventos específicos del sistema.
    - Deberá proporcionar múltiples niveles de privilegio para el usuario (solo lectura, según ubicación física edificio, planta, etc. capacidad de programar órdenes de trabajo, acceso a los informes, etc.)
    - El Deberá proporcionar capacidades de informes basados en web. Esta función debe permitir que los informes sean personalizables y se generen automáticamente en función de un calendario predefinido para su distribución a grupos de destinatarios predefinidos.
    - Deberá contar con una interfaz de aplicación API para poder integrarse con otras herramientas.
- Seguridad: La monitorización de la red también deberá incluir la detección de intrusiones y amenazas de seguridad. Deberá alertar sobre actividades sospechosas o patrones de tráfico malicioso, a través de un sistema de la herramienta de gestión de logs propiedad de la AEMET. Adicionalmente, la adjudicataria deberá enriquecer esta capacidad con un servicio de análisis de vulnerabilidades sobre todos los activos del Anexo I, que realice la identificación mediante una planificación y cuya identificación no suponga la disposición de ventanas de intervención al efecto. No se admitirán soluciones de escaneado para evitar la detención de los sistemas en producción.
- Escalabilidad: Los servicios de monitorización de la red deben ser escalables para adaptarse al crecimiento de la red. Deben ser capaces de gestionar y analizar grandes volúmenes de datos a medida que la red se expande.
- Integración: Es importante que el servicio se integre con otros sistemas de gestión de red y herramientas de automatización para permitir una administración más eficiente.
- Cumplimiento y registro: La monitorización de la red a menudo se utiliza para cumplir con requisitos regulatorios y para mantener registros de la actividad de la red, lo que puede ser crucial en las investigaciones de seguridad o auditorías que emprende AEMET.

La monitorización del estado de los elementos y servicios de red se realizará de manera centralizada y redundante desde el Centro de Operaciones en Redes (NOC) del adjudicatario (NOC) y desde SSCC de AEMET a través de las respectivas consolas.

Respecto de las características que debe cumplir el centro de soporte remoto (NOC):

- Prestación de los servicios en un modelo continuado (24x7)
- Cualificación para la prestación
- Operación y administración de sistemas de redes comunicaciones y plataformas de soporte a la operación TIC.

- Operación y administración de sistemas de protección perimetral, control de acceso a la red, etc....
- Operación y administración de sistemas de gestión de recursos y servicios LAN (Filtrado de Contenidos, Gestión de Ancho de Banda, distribución de rangos IPS control de usuarios, etc.)
- Gestión de incidentes (Redes, Comunicaciones, Seguridad, Sistemas, Aplicaciones)
- Contención y remediación coordinada con el equipo in situ.
- Auditoría de Red y Sistemas.
- Auditorías de seguridad.
- Auditoría normativa (RGPD/ISO/ENS)
- El centro de soporte del adjudicatario debe apoyarse en procedimientos reglados por las recomendaciones y cumplimientos obligados y teniendo en consideración las buenas prácticas recomendadas por ITIL4 V3, debiendo disponer de manera obligatoria de las siguientes certificaciones:
- UNE-EN ISO 20000 Certificado de Sistemas de Gestión de Servicio de Tecnologías de la Información.
- ISO 27001 de Gestión de la Seguridad de la Información.
- Esquema Nacional de Seguridad (ENS) con categoría alta.
- Membresía CSIRT.es
- Certificado CERT Coordination Center autorizado por Carnegie Mellon University
- Ser miembro de la comunidad FIRST (Forum of Incident Respones and Security Teams)
- Ser miembro de la Red Nacional de SOCs, con categoría GOLD.

4.3 Servicio de bolsa de horas

Con el objetivo de poder reforzar el servicio tanto en horario normal como en horario extendido (24x7x365), el adjudicatario deberá proveer una bolsa de horas tanto para la atención de incidentes (aportando técnicos adicionales a los que están asignados al servicio) como para la realización migración u otras actividades que por sus características deban restringirse a las horas de menor impacto en el servicio. Esta bolsa de horas tendrá una duración mínima de **60 horas / año**, corriendo por cargo del adjudicatario todos los costes de desplazamiento. Esta bolsa de 60 horas se subdivide a su vez 30 horas para atención de SSCC, y 30 horas para atención de Delegaciones Territoriales, aeropuertos, y demás ubicaciones (periferia).

4.4 Servicio de realización de pilotos

Ante la necesidad de implementar nuevas tecnologías, funcionalidades o elementos en la red de AEMET, el adjudicatario deberá realizar un análisis de idoneidad de las diferentes soluciones de los fabricantes en base a los pilotos que hayan presentado y a las necesidades y circunstancias específicas de la infraestructura de red de AEMET.

El número máximo de pilotos amparado en este punto será de **5 lo largo de cada año de duración del contrato y sus posibles prorrogas**, y su desarrollo deberá tener como objetivo la evaluación del rendimiento, de la confiabilidad y de la viabilidad antes de una implantación a gran escala, a través de las siguientes tareas de orden principal:

- Definición de objetivos y alcance:
    - Establecer claramente los objetivos de la experiencia piloto.
    - Delimitar el alcance de la experiencia piloto, incluyendo los dispositivos específicos que se van a probar y las áreas de la red involucradas.
- Selección de dispositivos y configuración:
    - Elegir los dispositivos de electrónica de red que se utilizarán en la experiencia piloto. Esto podría incluir enrutadores, switches, servidores, dispositivos de seguridad, etc.

    - Configurar los dispositivos de acuerdo con los requisitos de la prueba y las necesidades de la red.
- Planificación y diseño de la topología:
    - Diseñar una topología de red que refleje el entorno real en el que se implementará la solución.
    - Configurar la interconexión de dispositivos y asegurarse de que la topología de red esté lista para la prueba.
- Pruebas y monitorización:
    - Realizar pruebas específicas de acuerdo con los objetivos de la experiencia piloto. Esto podría incluir pruebas de rendimiento, pruebas de seguridad, pruebas de carga, entre otras.
    - Monitorizar continuamente el funcionamiento de los dispositivos y la red durante la prueba para detectar problemas y recopilar datos.
- Recopilación de datos y análisis:
    - Registrar los datos y resultados de las pruebas en detalle. Esto incluye métricas de rendimiento, problemas detectados y cualquier anomalía.
    - Realizar un análisis en profundidad de los datos recopilados para evaluar el rendimiento de los dispositivos y la capacidad de la red para cumplir con los requisitos.
- Identificación y resolución de problemas:
    - Si se encuentran problemas durante la experiencia piloto, identificar sus causas y trabajar en soluciones.
    - Ajustar la configuración de los dispositivos y de la red según sea necesario para abordar los problemas detectados.
- Documentación y elaboración de informes:
    - Crear un informe detallado que resuma los hallazgos de la experiencia piloto, incluyendo los resultados de las pruebas, los problemas encontrados y las soluciones aplicadas.
    - Recopilar recomendaciones para la implementación a gran escala o ajustes futuros.
- Ayuda a la toma de decisiones:
    - Basándose en los resultados de la experiencia piloto, prestar asistencia a la Dirección Técnica de AEMET en su proceso de toma de decisiones sobre si proceder con la implementación a gran escala de los dispositivos y soluciones probados.

4.5 Servicio de transferencia tecnológica

La empresa adjudicataria se comprometerá a impartir un mínimo de **25 horas/año** de formación grupal en las dependencias de AEMET, a un máximo de 10 técnicos de AEMET, en concepto de transferencia tecnológica, destinada a dotar a dicho personal técnico de los conocimientos necesarios sobre los procedimientos, métodos, herramientas y productos desarrollados o utilizados en el ámbito del proyecto, para dar soporte de primer nivel (diagnóstico y resolución de problemas simples).

La formación tendrá el alcance correspondiente a las implantaciones que la propia adjudicataria realice en el desempeño de los servicios que son objeto de esta contratación. Se incluirá la certificación oportuna que valide la asimilación del conocimiento por parte de los técnicos de AEMET que participen en la formación.

Los licitadores deberán definir los contenidos de los cursos propuestos conforme a los siguientes objetivos de aprendizaje:

1. Introducción a la tecnología que se incorpora.
2. Identificación de los dispositivos y/o servicios que se incorporan para desarrollar la tecnología.
3. Configuración y gestión de los activos involucrados.

4. Aspectos reseñables de seguridad de red que son incorporados.
5. Prácticas de laboratorio.
6. Pruebas de superación del conocimiento transferido.

5. CAPACIDAD DEL EQUIPO DE TRABAJO ASIGNADO POR LA ADJUDICATARIA

Para una correcta realización de las tareas que comprenden los diferentes servicios, los licitadores deberán justificar la asignación de un equipo de profesionales que cumplan con la cualificación y experiencia suficientes en el desempeño de las actividades que asumirán.

Se detalla en este apartado los mínimos exigibles que los licitadores deberán detallar en sus propuestas.

Las capacidades del personal que prestará el servicio serán acreditados por la empresa previamente a la adjudicación.

5.1 Horario para la prestación del servicio in situ

Este servicio se regirá por el de las oficinas de los servicios centrales de AEMET, en jornadas de 8 horas diarias: de 09 a 17 h (hora oficial peninsular) de lunes a viernes.

5.2 Lugar de prestación del servicio in situ

Por la especificidad de los servicios a contratar, la empresa adjudicataria destacará en la Sede Central de AEMET los recursos necesarios para la correcta prestación de estos.

El personal técnico de la empresa adjudicataria que acuda a las instalaciones de AEMET, no compartirá el mismo espacio físico que los funcionarios.

Los recursos materiales (teléfono móvil, ordenador personal, etc.) necesarios para prestar el servicio por parte del personal técnico del adjudicatario deberán ser aportados por el mismo.

La Sede Central de AEMET se encuentra en:

C/ Leonardo Prieto Castro 8 (Ciudad Universitaria) - 28040 Madrid

5.3 Composición del equipo asignado para el servicio in situ

5.3.1 Coordinador del equipo

El perfil propuesto deberá caracterizarse por su capacidad en los siguientes ámbitos:

- Habilidades de Comunicación: debe ser un comunicador efectivo, con habilidades excelentes tanto en la comunicación verbal como escrita, y ser capaz de transmitir información de manera clara y precisa.
- Planificación y Organización: debe ser capaz de organizar y coordinar eficazmente actividades de lanzamientos de proyectos o servicios.
- Conocimiento en Medios y Plataformas: debe estar al tanto de las últimas tendencias y desarrollos en las tecnologías objeto del contrato.
- Gestión de Proyectos: debe ser capaz de gestionar proyectos de redes de datos, estableciendo objetivos, plazos y recursos necesarios para llevar a cabo actividades de mantenimiento con éxito.
- Monitorización y Análisis: debe realizar seguimiento y análisis de las estrategias relacionadas con la evolución de la red de comunicaciones, para evaluar su eficacia.

Esto puede incluir el uso de métricas y análisis de datos para medir el impacto de las intervenciones sobre la red.
- Creatividad: se valorará su capacidad para desarrollar estrategias que impulsen la mejora de la red de comunicaciones.
- Capacidad para Trabajar en Equipo: deberá colaborar con otros departamentos y servicios, por lo que deberá poder trabajar en un entorno colaborativo.
- Adaptabilidad: deberá ser flexible y capaz de adaptarse a cambios en el entorno tecnológico, según convenga a la dirección estratégica.
- Ética Profesional: deberá mantener altos estándares éticos en el tratamiento de la confidencialidad, asegurándose de que la información proporcionada sea precisa y confiable.
- Manejo de Crisis: deberá prestar su colaboración en situaciones de crisis, participando en la comunicación de la organización, velando por su reputación.

Los niveles de cumplimiento del perfil requerido serán, como mínimo, los siguientes:

- Estar en posesión del título de Ingeniería Superior, o MECES III en ingeniería.
- Experiencia de más de diez años en jefatura de proyectos de redes de telecomunicaciones y/o seguridad de redes de telecomunicaciones.
- Dos certificaciones Cisco de entre las siguientes:
  - CCNA.
  - CCNP.
  - Cisco Certified Specialist.
  - CCIE.
- Certificación F5:
  - F5 Certified Administrator BIG-IP.
- Certificación ITIL.

5.3.2 Arquitecto de redes de comunicaciones

El perfil propuesto deberá caracterizarse por su capacidad en los siguientes ámbitos:

- Amplios Conocimientos Técnicos: debe tener un profundo conocimiento técnico en redes de telecomunicaciones, incluyendo protocolos, tecnologías de red, enrutadores, switches, protocolos de enrutamiento, topologías de red, seguridad de red y más.
- Diseño de Redes Complejas: deberá tener capacidad para evaluar redes complejas que sean escalables, seguras y eficientes para cumplir con los requisitos de AEMET. Esto implica la creación de planos de red detallados y la selección de componentes adecuados.
- Resolución de Problemas: deberá ser capaz de enfrentar desafíos técnicos significativos, como la identificación y solución de cuellos de botella de rendimiento, problemas de seguridad, o la optimización de redes.
- Conformidad con Estándares y Regulaciones: deberá asegurarse de que la red cumpla con los estándares y regulaciones de la industria, especialmente en lo que respecta a la seguridad y la privacidad de los datos.
- Seguridad de Red: la seguridad es una prioridad, por lo que deberá ser capaz de diseñar sistemas de seguridad efectivos, implementar cortafuegos, sistemas de detección de intrusiones y aplicar políticas de seguridad de red.
- Evaluación de Tecnologías Emergentes: deberá estar al tanto de las tecnologías emergentes en el campo de las telecomunicaciones y evaluar si estas tecnologías pueden aportar mejoras a la infraestructura de red existente.
- Comunicación Efectiva: la capacidad de comunicarse de manera efectiva con colegas, superiores y otros equipos es esencial, especialmente en el ámbito de la tecnología.
- Habilidades de Gestión de Proyectos: deberá poseer habilidades de gestión de proyectos para garantizar que los proyectos se completen a tiempo y dentro del presupuesto.

- Visión Estratégica: deberá aportar una visión estratégica para planificar la evolución de la red a largo plazo, anticipando las necesidades futuras de la organización y las tendencias tecnológicas.
- Colaboración: Deberá facilitar su colaboración con otros departamentos, como el de TI, seguridad, y desarrollo de aplicaciones, para asegurar que las redes se integren con el resto de los servicios de AEMET.
- Documentación Rigurosa: deberá colaborar en la construcción de documentación detallada de diseños, configuraciones y procedimientos es esencial para garantizar la eficiencia y la capacidad de respuesta en caso de problemas.

Los niveles de cumplimiento del perfil requerido serán, como mínimo, los siguientes:

- Titulación de ciclo formativo superior de carácter tecnológico.
- Experiencia de al menos siete años en proyectos de redes de telecomunicaciones y/o seguridad de redes de telecomunicaciones.
- Al menos una certificación de entre:
  - Cisco CCNP.
  - Cisco Certified Specialist - Security Core.
- Al menos dos certificaciones de entre las siguientes:
  - Fortinet NSE 4.
  - Fortinet NSE 5.
  - Fortinet NSE 7.
- Una certificación sobre soluciones NAC de entre los siguientes fabricantes:
  - Fortinet.
  - Extreme Networks.
  - Cisco.

5.3.3 Técnico de redes de comunicaciones (4)

Se requiere un mínimo de CUATRO TÉCNICOS que deberán caracterizarse por su capacidad en los siguientes ámbitos:

- Conocimiento Técnico: deberá tener un sólido conocimiento técnico en redes de telecomunicaciones, incluyendo protocolos, tecnologías de red, enrutadores, switches, cables, conectividad, protocolos de enrutamiento y topologías de red.
- Resolución de Problemas: deberá aportar experiencia en la identificación y resolución de problemas en las redes.
- Configuración de Dispositivos de Red: como responsable de configurar y mantener dispositivos de red (enrutadores, switches, cortafuegos, puntos de acceso inalámbrico, etc.) deberá ser capaz de asegurar que estos dispositivos funcionen correctamente y cumplan con las políticas de seguridad de AEMET.
- Seguridad de Red: deberá implementar políticas de seguridad, cortafuegos y sistemas de detección de intrusiones para proteger la red contra amenazas cibernéticas.
- Pruebas y Monitorización: para realizar pruebas de rendimiento y monitorización del tráfico de la red, en orden de garantizar un funcionamiento eficiente y detectar problemas de manera proactiva.
- Documentación: deberá colaborar en la redacción técnica de la configuración de la red, procedimientos y cambios realizados en la red, para el seguimiento y la resolución de problemas.
- Comunicación Efectiva: deberá ser capaz de comunicarse de manera efectiva con los usuarios finales y otros miembros del equipo técnico. La capacidad para explicar problemas técnicos de manera comprensible es esencial.
- Colaboración: para trabajar en estrecha colaboración con otros miembros del equipo de TI, como administradores de sistemas, arquitectos de redes y profesionales de seguridad de TI, en orden de garantizar que la infraestructura de red sea coherente y se integre con otras operaciones de TI.

- Disponibilidad y Respuesta a Emergencias: deberá tener disponibilidad para ser llamado a responder a problemas de red en situaciones de emergencia, por lo que deberá colaborar en la resolución de problemas críticos.

Los niveles de cumplimiento de los perfiles requeridos serán, como mínimo, los siguientes:

- Titulación de ciclo formativo superior de carácter tecnológico.
- Al menos uno de los técnicos deberá aportar experiencia de cinco años en proyectos de redes de telecomunicaciones y/o seguridad de redes de telecomunicaciones.
- Todos los técnicos deberán aportar experiencia de dos años en proyectos de redes de telecomunicaciones y/o seguridad de redes de telecomunicaciones.
- Al menos dos técnicos deberán aportar una certificación de entre:
  - Cisco CCNA.
  - Cisco CCNP.
- Al menos uno de los técnicos deberá aportar una certificación de entre las siguientes:
  - Fortinet NSE3.
  - PaloAlto PCNSE.
  - F5 Certified Administrator BIG-IP.
- Al menos uno de los técnicos deberá aportar su certificación "SYSTIMAX Installation & Maintenance"

5.4 Política de reemplazos para el equipo asignado in situ

Respondiendo al objeto del contrato, se requiere que la adjudicataria garantice la estabilidad del personal asignado para asegurar la realización con éxito de las actividades periódicas y recurrentes. La incorporación, sustitución o baja del cualquiera de los integrantes de los equipos, requerirá la aprobación de la Dirección Técnica de AEMET.

La empresa adjudicataria garantizará que las personas que componen los equipos de trabajo mantendrán una permanencia mínima en el proyecto de **seis meses**. Asimismo, tendrá, a lo largo de la duración del contrato, un número de personas formadas con vistas a una posible sustitución inmediata.
Si la firma adjudicataria propusiera el cambio de una de las personas del equipo de trabajo, lo deberá solicitar por escrito con quince días de antelación, exponiendo las razones que obligan a la propuesta.

La incorporación adicional de nuevos recursos al equipo de trabajo habrá de solicitarse con un preaviso de **quince días**.

6. DURACIÓN

El contrato tiene una duración de **VEINTICUATRO MESES**, con una posible prórroga de DOCE meses adicionales.

7. CONDICIONES GENERALES

El objeto del contrato es el establecido en el apartado 2 de este PPT con el alcance definido en el apartado 4.

Al inicio del servicio, es requisito indispensable la realización de una auditoría inicial de la infraestructura de red LAN y comunicaciones de todos los sistemas actuales disponibles en la red del AEMET.

El servicio incluye además el mantenimiento de los elementos y servicios de red que se catalogan en el ANEXO I y que no disponen de garantía del fabricante durante la extensión prevista del contrato o su posible prórroga.

Los diferentes Servicios relacionados en este pliego (con la excepción del Servicio de transferencia tecnológica) estarán disponibles en todos sus puntos de acceso 24 horas al día todos los días del año.

Por la especificidad de los servicios a contratar (administración y gestión de sistemas críticos incluyendo resolución de incidencias in situ, comprobación de los entornos antes y después de actualizaciones de software de base, configuración y pruebas, formación del personal técnico de AEMET, reuniones de seguimiento y control, y cualquier situación de emergencia en los sistemas a administrar) la empresa adjudicataria destacará en la Sede Central de AEMET los recursos necesarios para la correcta prestación de los mismos. Así, los servicios serán prestados por el adjudicatario de la siguiente forma:

- **Servicios in situ (apartado 4.1)**:

  en horario de oficina (laborables, de 09 a 17 horas): desde los Servicios Centrales (SSCC) de AEMET, atendiendo desde allí de manera presencial la planta de SSCC y del resto de sedes de AEMET en remoto.

- **Servicios no in situ (apartado 4.2)**:

  Fuera de horario de oficina (horario 24 x 7), el adjudicatario mantendrá los servicios objeto de contrato en horario continuado desde su centro de operaciones de red (NOC), en monitorización y control remotos.

- **Servicio de bolsa de horas (apartado 4.3):**

  SSCC: Se complementarán las actividades presenciales en SSCC y adicionales a los servicios in situ de gestión y mantenimiento que se deban realizar fuera de horario de oficina (tanto causadas por incidentes como por la ejecución de mejoras que supongan un corte en la red)

  Sedes diferentes a SSCC, fuera de la Comunidad de Madrid y detallados en el Anexo I. Dentro de esta bolsa no se incluyen los tiempos de desplazamiento. Su objetivo es la realización de tareas de asistencia y soporte sin coste, de un técnico de movilidad (ajeno a los que prestan servicio en SSCC de Madrid), para las intervenciones in situ en dichas sedes. El adjudicatario cubrirá todos los gastos que se deriven del cumplimiento de estos servicios, incluidos los desplazamientos y dietas.

El personal técnico de la empresa adjudicataria que acuda a las instalaciones de AEMET, no compartirá el mismo espacio físico que los funcionarios.

Los recursos materiales necesarios para prestar el servicio por parte del personal técnico del adjudicatario deberán ser aportados por el mismo.
La dirección de la Sede Central de AEMET es:

C/Leonardo Prieto Castro 8
28040 – Madrid

El oferente podrá establecer y costear (incluyendo la instalación y el uso) una conexión con los equipos de los sistemas, que permita diagnosticar y, en su caso, solucionar las incidencias que se presenten, en remoto (se admite vía VPN), desde su NOC.

El adjudicatario establecerá, sin coste adicional, los bancos de prueba y/o instalaciones piloto que puedan requerirse por parte de AEMET para la elaboración de los estudios e informes técnicos de evaluación que aseguren las condiciones técnicas y de servicio establecidas en este Pliego.

AEMET podrá sustituir a lo largo del periodo de ejecución del contrato, equipos relacionados en el Anexo I. Por tanto, el adjudicatario aceptará la sustitución de algunos de estos equipos por otros de la misma funcionalidad. Estas variaciones del parque contratado no suponen modificación del servicio objeto de este contrato (incluso pueden tener lugar a lo largo de la tramitación de este expediente), sino de la aplicación de dicho servicio a elementos diferentes de los relacionados en el ANEXO I, siempre que se mantengan la misma o análoga funcionalidad y su cantidad.

En caso ineludible para AEMET de tener que **incorporar nuevo equipamiento** (similar al relacionado en el ANEXO I) y **adicional** al contrato, a causa de cambios introducidos en la estructura de red o el entorno tecnológico, el adjudicatario debe comprometerse a asumir variaciones en el número de equipos soportados y mantenidos, en las siguientes cantidades:

- **Equipamiento de Servicios Centrales**: El ubicado en SSCC, salvo los conmutadores de planta. Se admitirá la inclusión adicional en soporte y gestión de garantías durante el contrato, de un **máximo de cinco equipos o sistemas adicionales**, ya sean físicos o virtuales, sin sobrecoste alguno.
- **Conmutadores de planta en SSCC y conmutadores en resto de sedes**: Se admitirá la inclusión adicional en soporte y mantenimiento de un **máximo del 10 % del total de estos equipos**, sin sobrecoste alguno.
- Para poder determinar en su caso los aumentos citados, el adjudicatario debe basarse en el inventario propuesto en este PPT (establecido en ANEXO I), actualizado a la fecha de la presentación de la oferta.

8. ACUERDO DE NIVEL DE SERVICIO (ANS)

La prestación de los servicios objeto de este contrato conlleva los compromisos de cumplimiento de los niveles mínimos de servicio recogidos en el este apartado. Su incumplimiento llevara aparejado las penalizaciones establecidas en los artículos 192 y 193 de Ley 9/2017, de 8 de noviembre de Contratos del Sector Público. Por tanto, el adjudicatario deberá contar con los medios propios, de toda índole (recursos humanos, de logística, distribución y almacenaje), necesarios para cumplir con lo exigido.

Además del acceso a la información a través del Sistema de Gestión del Servicio requerido, el adjudicatario entregará la información relativa a incidencias en formato HTML, Excel, Word, o similar con periodicidad mensual. A solicitud del Director Técnico del proyecto (nombrado por AEMET), el adjudicatario elaborará informes específicos y detallados sobre las incidencias más graves, y los presentará a la mayor brevedad. Finalmente, y de manera trimestral se entregará al AEMET un informe con las estadísticas de uso y las acciones de mantenimiento realizadas sobre cada uno de los equipos.

El adjudicatario comunicará al Director Técnico de AEMET, vía correo electrónico, las paradas previstas por actividades de mantenimiento programado con un mínimo de 48 horas de antelación. En el caso de las actuaciones que afecten a ENAIRE la antelación con que se avise debe ser de 5 días. Estos periodos, no computarán para el cálculo de penalizaciones.

La duración de la fase de implantación, durante la cual el servicio podrá no cumplir algunos de los niveles acordados, no podrá superar los 2 meses de duración contados a partir de la firma del contrato.

El oferente mantendrá un horario de acceso a su servicio de gestión de incidencias y soporte de 7x24x365.

La recepción administrativa de una incidencia será inmediata. El tiempo de respuesta lo determinará la recepción de la incidencia, entendiendo por tal su toma de razón por un técnico evaluador o responsable de la misma. A partir de la recepción de la incidencia todo el tiempo empleado en exploraciones diagnósticas previas apoyadas o no por técnicos de AEMET será contabilizado como tiempo de resolución.

En caso de no resolverse la incidencia de otro modo, deberá personarse un técnico de mantenimiento en la sede donde esté instalado el equipo averiado, en los tiempos reflejados en la siguiente Tabla. En el ANEXO I se relacionan los diferentes equipos **adscritos a cada criticidad**, así como su ubicación.

CRITICIDAD	TIEMPO RESPUESTA	TIEMPO PRESENC. INSTALACION
MAXIMA	Antes de 1 hora	Antes de 4 horas
MEDIA	Antes de 1 hora	Antes de 6 horas

Las averías e incidencias tienen su reflejo en el nivel de servicio proporcionado por cada equipo o sistema. A efectos de penalizaciones, el servicio proporcionado se clasifica en:

NIVEL SERVICIO	DESCRIPCIÓN
NORMAL	El servicio se presta con el nivel normal
DEGRADADO	Rendimiento inferior, o sin respaldo, o fallo parcial de un equipo
FALLO TOTAL	Rendimiento inaceptable o nulo del servicio

El tiempo de resolución de avería es el que transcurre entre la comunicación de la recepción de la avería por el técnico responsable o evaluador y la restauración funcional del servicio, ya sea por reparación, por reconfiguración o por sustitución de equipo o parte del equipo, de cualquier modo que ésta se produzca. Dependiendo de la criticidad será:

CRITICIDAD	TIEMPO DE RESOLUCION DE AVERIA (TR)
MAXIMA	Antes de 6 horas (TANS)
MEDIA	Antes de 12 horas(TANS)

9. SISTEMA DE GESTIÓN DEL SERVICIO

9.1 Introducción

Dado el volumen y la complejidad de la información asociada a los servicios solicitados, AEMET deberá disponer de un Sistema de Gestión del Servicio (SGS) para la gestión de las actualizaciones asociadas al tráfico, alarmas, configuración, incidencias y monitorización de los niveles de servicio solicitados en este expediente, que será accesible desde AEMET y desde el Centro de Gestión del Adjudicatario.

Los licitadores deberán presentar en su oferta una descripción detallada de su propuesta para el mantenimiento del Sistema de Gestión, cumpliendo individualmente con cada uno de los requisitos y funcionalidades que a continuación presentamos.

9.2 Funcionalidades del SGS

El Sistema de Gestión del Servicio (SGS) deberá ser un sistema abierto que proporcione accesos a la información gestionada, de modo que pueda ser accedida, actualizada y exportada a otros sistemas de AEMET. No se admitirán soluciones propietarias o que precisen licencias para el intercambio de datos con la plataforma del cliente.

El SGS permitirá obtener toda la información necesaria para la administración de las redes de AEMET (inventario, configuraciones, alarmas, gestión de incidencias) proporcionando informes y estadísticas, manteniendo una base de datos, relacional y abierta de los elementos gestionados.

El SGS deberá disponer de medidas de autenticación para asegurar que pueda ser utilizado solamente por usuarios autorizados de AEMET, y con acceso a los datos que correspondan según el perfil del usuario.

El sistema debe ser accesible vía Web desde Internet mediante el protocolo HTTPs y con validación de la IP origen.

El SGS deberá notificar de la recepción de cualquier transacción con indicación de fecha y hora.

La funcionalidad mínima que debe ofrecer el SGS será:

- Gestión de Administración: Inventario de equipamiento, control de versiones, servicios asociados, conexiones a la LAN y a la WAN, diagramas físicos y lógicos de red, direccionamiento, licencias y garantías, etc.
- Gestión de la Seguridad: Monitorización de la seguridad en el equipamiento monitorizado por el SIEM, operación de la plataforma, administración de la plataforma y seguimiento de incidencias desde la apertura al cierre
- Gestión de la Configuración: Visualización parámetros de configuración de cada equipo, backup activos, etc.
- Gestión de Incidencias: Comunicación de incidencias (formularios en línea), incluyendo diagnóstico, medidas correctoras para su resolución y plazo estimado. El SGS gestionará incidencias de los sistemas y redes se AEMET que son responsabilidad directa del adjudicatario, así como incidencias de las redes WAN a las que está conectado AEMET y que se hayan detectado por el adjudicatario o tramitado a través de este
- Gestión del Rendimiento (prestaciones): mediar, cuantificar, analizar y controlar las prestaciones de los distintos componentes de red para poder ajustar los parámetros de la red
- Cuadro de Mando: Resúmenes ejecutivos sobre cargas de los sistemas, accesos, incidencias, estado de la red, etc.
- Gestión de la disponibilidad: monitorización del estado operativo de cada servicio y/o equipo mantenido, definición de umbrales, diseño de alarmas, avisos de caída, intrusiones y ataques ordenados por gravedad del fallo

El servicio SGS ha de estar disponible y plenamente operativo 1 mes después de la firma del contrato.

10. GESTIÓN DEL PROYECTO

Dirección: Corresponde a AEMET el control, la supervisión y la dirección del proyecto, así como proponer las modificaciones que convenga introducir. Para ello, designará un Director Técnico cuya función principal, en relación con el objeto del presente proyecto, será velar por el cumplimiento de los servicios exigidos y ofertados. El Director Técnico podrá delegar sus funciones en una persona de su equipo.

Asimismo, podrá incorporar al proyecto durante su realización las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo.

La valoración final de la productividad y calidad de los servicios prestados por los técnicos aportados por la empresa adjudicataria corresponde al Director Técnico de AEMET. Otras funciones del Director Técnico serán las siguientes:

- Velar por el cumplimiento de los servicios exigidos y ofertados.
- Emitir las certificaciones necesarias para los pagos de los servicios.

Coordinador del Equipo: El adjudicatario designará una persona como Coordinador del Equipo para el Proyecto que asumirá las funciones de interlocución con el Director Técnico de AEMET, así como las tareas de coordinación y dirección del proyecto dentro de su empresa con el perfiles técnico y con la experiencia indicada en apartado 5.3 y subapartados de este PPT para este perfil.

Los contactos directos de las personas del equipo de trabajo de la empresa adjudicataria con el usuario final, no se realizarán sin el conocimiento previo y autorización del Director Técnico de AEMET.

Resto de efectivos del equipo de trabajo: Se estima que el adjudicatario, para la prestación del servicio solicitado en este pliego, necesita proveer los efectivos mínimos y con los perfiles técnicos y con la experiencia indicada en apartado 5.3 y subapartados de este PPT, tanto en su modalidad in situ como no in situ.

La falsedad en el nivel de conocimientos técnicos exigidos en este pliego del personal dedicado por el adjudicatario, deducida los conocimientos reales demostrados en la ejecución de los trabajos, implicará asumir las penalizaciones especificadas en el PCAP.

El adjudicatario se comprometerá a incorporar las personas ofertadas al equipo de trabajo al día siguiente a la firma del contrato.

11. CALIDAD

En las ofertas se deberán especificar las medidas de control que se tomarán en caso de ser adjudicatarias para asegurar la calidad del servicio a prestar, por lo que la misma deberá contener un Plan de Aseguramiento de la Calidad.

La Gestión de la Calidad consistirá en el conjunto de tareas y funciones que realizará la empresa adjudicataria para garantizar que el proyecto se realiza de acuerdo al plan establecido y con el alcance definido.

12. DETERMINACIÓN DEL PRECIO

Se ha realizado la correspondiente prospección de mercado, para la evaluación del precio de licitación del presente expediente, según los siguientes conceptos coherentes con el presente Pliego de Prescripciones Técnicas:

Concepto	Observaciones	Coste Estimado
Servicios in situ de gestión y mantenimiento de redes LAN	Soporte 8x5 • Monitorización de la red LAN • Gestión de incidencias • Implementación de las medidas e iniciativas de seguridad definidas por la OTS • Gestión de la configuración y administración del conjunto de equipos de infraestructura de red • Gestión de inventario de equipos y sistemas • Gestión de garantías y soporte del fabricante • Gestión del mantenimiento • Control del cableado y otros elementos de acceso. Etiquetado y certificación	1.159.657,75 €
Servicios no in situ	Soporte 24x7x365 Función de monitorización remota. Servicios NOC (remoto)	155.162,54 €
Servicio realización de pilotos	5 servicios lo largo de cada año de duración del contrato y sus posibles prorrogas 80 horas anuales Precio según estimación de mercado	5.500,00 €
Servicio de bolsa de horas	60h/año 24x7x365	8.446,42 €
Servicio de transferencia tecnológica	Formación reglada 25h/por año de contrato Precio según estimación de mercado	6.875,00 €
Suministros: a) Agente VPN b) herramienta de gestión de FortiClient (EMS)	Soporte NBD 24x7, 5 años	56.814,33 €
Suministros: Herramienta de gestión de cableado	Licencia hasta 1000 puntos de red	32.288,52 €
Suministros: Herramienta de análisis de tráfico	Licencia para gestión de 300 dispositivos	69.857,36 €

TOTAL: 1.494.601,92 € (1.808.468,32 € IVA incluido)

La justificación y el desglose de este presupuesto se encuentra en el ANEXO III de este PPT.

14. TRANSFERENCIA TECNOLÓGICA y FORMACIÓN

Durante la ejecución de los trabajos objeto del contrato el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por el Centro Directivo a tales efectos, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizados para resolverlos.

15. DOCUMENTACIÓN DE LOS TRABAJOS

Como parte de los trabajos objeto del contrato, el adjudicatario se compromete a generar para cada procedimiento establecido, auditoria de prestaciones o consultoría de evolución, toda la documentación que sea aplicable, a solicitud del Director Técnico. La documentación, quedará en propiedad exclusiva de AEMET sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de este centro directivo, que la daría en su caso previa petición formal del contratista con expresión del fin. La documentación será facilitada en soporte electrónico.

Madrid, a la fecha de la firma electrónica

EL COORDINADOR DE TELEMÁTICA

Jesús Manuel Montero Garrido

CONFORME

EL DIRECTOR DE PRODUCCIÓN E INFRAESTRUCTURAS

Jaime Rey Vidaurrázaga

ANEXO I – SISTEMAS Y EQUIPOS DENTRO DEL OBJETO DEL CONTRATO

Por motivos de protección, para obtener acceso al contenido de este anexo debe cumplimentarse y firmarse digitalmente ANEXO IV – PETICIÓN DE ACCESO A ANEXO I Y ANEXO II y enviarse a jmonterog@aemet.es

ANEXO II – ESQUEMA GENERAL DE LA RED DE AEMET

Por motivos de protección, para obtener acceso al contenido de este anexo debe cumplimentarse y firmarse digitalmente ANEXO IV – PETICIÓN DE ACCESO A ANEXO I Y ANEXO II y enviarse a jmonterog@aemet.es

ANEXO III – DESGLOSE DEL PRESUPUESTO DE LICITACIÓN

1. Objeto

En el presente anexo desglosa el presupuesto de la licitación "SERVICIOS DE GESTIÓN DE RED PARA LA AGENCIA ESTATAL DE METEOROLOGÍA" en costes directos, indirectos y otros costes, y detalla el método de cálculo de los servicios incluidos

La contratación de estos servicios no implica participación directa de la empresa adjudicataria en el ejercicio de las potestades públicas ni en la salvaguardia de los intereses generales del Estado y de las Administraciones Públicas, ni tampoco consiste en la realización de funciones propias de secretaría, unidad de apoyo o registro.

Se reproduce la tabla de servicios y suministros presupuestados, disponible en el epígrafe 12 del pliego de prescripciones técnicas:

Concepto	**Observaciones**	**Coste Estimado**
Servicios in situ de gestión y mantenimiento de redes LAN	Soporte 8x5 • Monitorización de la red LAN • Gestión de incidencias • Implementación de las medidas e iniciativas de seguridad definidas por la OTS • Gestión de la configuración y administración del conjunto de equipos de infraestructura de red • Gestión de inventario de equipos y sistemas • Gestión de garantías y soporte del fabricante • Gestión del mantenimiento • Control del cableado y otros elementos de acceso. Etiquetado y certificación	1.159.657,75 €
Servicios no in situ	Soporte 24x7x365 Función de monitorización remota. Servicios NOC (remoto)	155.162,54 €
Servicio realización de pilotos	5 servicios lo largo de cada año de duración del contrato y sus posibles prorrogas 80 horas anuales Precio según estimación de mercado	5.500,00 €
Servicio de bolsa de horas	60h/año 24x7x365	8.446,42 €
Servicio de	Formación reglada	6.875,00 €

transferencia tecnológica	25h/por año de contrato Precio según estimación de mercado	
Suministros: a) Agente VPN b) herramienta de gestión de FortiClient (EMS)	Soporte NBD 24x7, 5 años	56.814,33 €
Suministros: Herramienta de gestión de cableado	Licencia hasta 1000 puntos de red	32.288,52 €
Suministros: Herramienta de análisis de tráfico	Licencia para gestión de 300 dispositivos	69.857,36 €

2. Cálculos relativos al presupuesto base de los SUMINISTROS

Concepto	CD	CI (5% CD)	CD + CI	GG (13% CD+CI)	BI (6% CD + CI)	Coste Estimado
Suministros: a) Agente VPN b) herramienta de gestión de FortiClient (EMS)	45.469,65 €	2.273,48 €	47.743,13 €	6.206,61 €	2.864,59 €	56.814,33 €
Suministros: Herramienta de gestión de cableado	25.841,15 €	1.292,06 €	27.133,21 €	3.527,32 €	1.627,99 €	32.288,52 €
Suministros: Herramienta de análisis de tráfico	55.908,25 €	2.795,41 €	58.703,66 €	7.631,48 €	3.522,22 €	69.857,36 €

3. Cálculos relativos al presupuesto base de los SERVICIOS

Concepto	CD	CI (5% CD)	CD + CI	GG (13% CD+CI)	BI (6% CD + CI)	Coste Estimado
Servicios in situ de gestión y mantenimiento de redes LAN	928.097,44 €	46.404,87 €	974.502,31 €	126.685,30 €	58.470,14 €	1.159.657,75 €
Servicios no in situ	124.179,70 €	6.208,99 €	130.388,69 €	16.950,53 €	7.823,32 €	155.162,54 €
Servicio realización de pilotos	4.401,76 €	220,09 €	4.621,85 €	600,84 €	277,31 €	5.500,00 €
Servicio de bolsa de horas	6.759,84 €	337,99 €	7.097,83 €	922,72 €	425,87 €	8.446,42 €
Servicio de transferencia tecnológica	5.502,20 €	275,11 €	5.777,31 €	751,05 €	346,64 €	6.875,00 €

a. Servicios según costes salariales

El resto de servicios se ha calculado estimando el número de técnicos necesarios para su satisfacción, calculándose los costes salariales a partir del XVIII Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública (Resolución de 13 de julio de 2023, de la Dirección General de Trabajo) y en función de la dedicación de los técnicos adscritos a la ejecución del contrato.

- **Coordinador del equipo**: Perfil Coordinador/Consultor. Aunque a disponibilidad permanente de AEMET, sus tareas son de índole administrativa, por lo que no se considera imprescindible la dedicación exclusiva al proyecto, estimándose suficiente una dedicación del 50% del tiempo. Se corresponde este perfil con Grupo A, nivel I, del área 3 del convenio referido anteriormente.
- **1 Arquitecto de redes de comunicaciones**: Trabajo in situ, horario de oficina. Este perfil deberá asesorar a AEMET ante posibles arquitecturas y evoluciones de las redes y comunicaciones en AEMET, por lo que se necesita un alto grado de especialización en soluciones de redes y comunicaciones. Se estima suficiente un 100% de dedicación a este proyecto. Se corresponde este perfil con Grupo A, nivel I, del área 4 del convenio referido anteriormente
- **4 Técnicos de redes de comunicaciones**: Trabajo in situ, horario de oficina, por la duración total del contrato (dedicación 100%). Se encargará del mantenimiento preventivo, correctivo, evolutivo y perfectivo de las redes e infraestructuras de comunicaciones objeto del contrato. Imprescindible alto grado de especialización en redes de comunicaciones e infraestructura de comunicaciones. Se corresponde este perfil con Grupo C, nivel I, del área 3 del convenio referido anteriormente.
- **2 Técnicos nivel N1**: Trabajo en remoto para la realización de las tareas no in situ. NOC en remoto (dedicación 45%). Es necesario un cierto de grado de especialización para atender las incidencias fuera de horario de oficina, pero su dedicación no es imprescindible sea exclusiva para AEMET. Se corresponde este perfil con Grupo C, nivel I, del área 3 del convenio referido anteriormente

Glosario:

Gastos directos (CD): Asociados a los costes de personal.

Gastos Indirectos (CI): Normalmente los fabricantes disponen de una plataforma de atención remota 24x7 tipo "SOC", cuyos costes/amortización son redundados en los clientes como gastos indirectos. Se calcula como un 5% de los costes directos.

Gastos generales (GG): Otros costes, propios de la empresa. Se calcula como un 13% de la suma de los costes directos y de los costes indirectos.

Beneficio industrial (BI): Se calcula como un 6% de la suma de los costes directos y de los costes indirectos.

Notas

(*) Se requiere personal con conocimientos, habilidades y destrezas específicos que conllevan que el personal que posee dichas competencias técnicas esté especialmente reconocido y valorado en el mercado laboral
[1] El cálculo del salario anual se ha estimado para un total de 1.760 horas/año
[2] Incremento estimado como consecuencia de la especialización del perfil
[3] Se ha estimado un 30% de coste de la Seguridad Social
[4] Calculado como un tanto por ciento (5%) de los costes directos (gastos de personal)
[5] Calculado como un tanto por ciento (13%) de la suma de los costes directos (gastos de personal) y de los costes indirectos
[6] Calculado como un tanto por ciento (6%) de la suma de los costes directos (gastos de personal) y de los costes indirectos
[7] Suma de los costes directos, costes indirectos, gastos generales y beneficio industrial
[8]Los gastos generales y el beneficio industrial son presentados conjuntamente como "Otros costes" tanto en el presente Anexo como en el Cuadro de características administrativas.

Costes de personal (anuales)										
Perfiles	***Dedicación***	***Salario Base***	***Plus Convenio***	***Salario actualizado***	***Especialización tecnológica (XX%)[1]***	***Salario anual***	***Coste anual según dedicación***	***FTEs***	***Coste personal contrato***	***Coste personal contrato con Seguridad Social 30%***
Coordinador del equipo	*50%*	26.540,58 €	*2.309,65 €*	*28.850,23 €*	*100%*	*57.700,46 €*	*28.850,23 €*	1	*28.850,23 €*	*37.505,30 €*
Arquitecto redes de comunicaciones	*100%*	26.592,86 €	*2.366,48 €*	*28.959,34 €*	*300%*	*115.837,36 €*	*115.837,36 €*	1	*115.837,36 €*	*150.588,57 €*
Técnico de redes de comunicaciones	*100%*	24.421,84 €	*2.112,28 €*	*26.534,12 €*	*100%*	*53.068,24 €*	*53.068,24 €*	4	*212.272,96 €*	*275.954,85 €*
Perfil N1 en remoto	*45%*	24.421,84 €	*2.112,28 €*	*26.534,12 €*	*100%*	*53.068,24 €*	*23.880,71 €*	2	*47.761,42 €*	*62.089,85 €*

Costes de personal por duración total de expediente:

Coste personal asociado servicio insitu (duracion total expediente)	928.097,44 €
Coste personal asociado servicio no insitu (duracion total expediente)	124.179,70 €
Costes persontal duracion total expediente	1.052.277,14 €

Desglose del presupuesto en Costes Directos, Indirectos y Otros Costes

Concepto	CD	CI (5%)	CD + CI	GG (13%)	BI (6%)	Coste Estimado
Servicios in situ de gestión y mantenimiento de redes LAN	928.097,44 €	46.404,87 €	974.502,31 €	126.685,30 €	58.470,14 €	1.159.657,75 €
Servicios no in situ	124.179,70 €	6.208,99 €	130.388,69 €	16.950,53 €	7.823,32 €	155.162,54 €
Servicio realización de pilotos	4.401,76 €	220,09 €	4.621,85 €	600,84 €	277,31 €	5.500,00 €
Servicio de bolsa de horas	6.759,84 €	337,99 €	7.097,83 €	922,72 €	425,87 €	8.446,42 €
Servicio de transferencia tecnológica	5.502,20 €	275,11 €	5.777,31 €	751,05 €	346,64 €	6.875,00 €
Suministros: a) Agente VPN b) herramienta de gestión de FortiClient (EMS)	45.469,65 €	2.273,48 €	47.743,13 €	6.206,61 €	2.864,59 €	56.814,33 €
Suministros: Herramienta de gestión de cableado	25.841,15 €	1.292,06 €	27.133,21 €	3.527,32 €	1.627,99 €	32.288,52 €
Suministros: Herramienta de análisis de tráfico	55.908,25 €	2.795,41 €	58.703,66 €	7.631,48 €	3.522,22 €	69.857,36 €

Presupuesto Desglosado

Lo que en conclusión da lugar a:

Desglose Precio	
Costes directos	
Personal	1.052.277,14 €
Resto costes directos	143.882,85 €
Costes Indirectos	59.808,00 €
Gastos Generales	163.275,85 €
Beneficio industrial	75.358,08 €
Total sin IVA	1.494.601,92 €

Donde:

- Costes Indirectos: Calculados como un tanto por ciento (5%) de los costes directos.
- Gastos Generales: Calculados como un tanto por ciento (13%) de la suma de los costes directos y de los costes indirectos
- Beneficio Industrial: Calculado como un tanto por ciento (6%) de la suma de los costes directos y de los costes indirectos

ANEXO IV – PETICIÓN DE ACCESO A ANEXO I Y ANEXO II

Nombre completo del solicitante:

Empresa:

Cargo o relación con la organización:

DNI/CIF:

Correo electrónico del solicitante:

Detalles de la Petición:

Acceso a ANEXO I y ANEXO II de PPT
de SERVICIOS DE GESTIÓN DE RED PARA LA AGENCIA ESTATAL DE METEOROLOGÍA

Fecha de la solicitud:

Justificación de la Petición:

Motivo de la solicitud de acceso:

[X] Preparación de oferta para licitación

Compromisos del Solicitante:

Compromiso de Confidencialidad:

Al firmar este formulario, el solicitante se compromete a tratar la información a la que se accede con la máxima confidencialidad y exclusivamente para el motivo de acceso.

Firma del solicitante: _____ Fecha: _____