Nota aclaratoria: En caso de duda o contradicción entre el original en catalán y la versión en castellano de este Pliego prevalecerá la versión en catalán.

PLIEGO DE PRESCRIPCIONES TÉCNIQUES PARA LA CONTRATACIÓN DEL SERVICIO DE MANTENIMIENTO Y ADMINISTRACIÓN DE LAS REDES DE DATOS DEL CONSORCI MAR PARC DE SALUT DE BARCELONA

1. Objetivo

1.1. Introducción

El objeto del contrato corresponde a la realización del servicio de mantenimiento y administración de las redes de datos de los Centros del Consorci Mar Parc de Salut de Barcelona.

El Consorci Mar Parc de Salut de Barcelona (CMPSB) ofrece servicios sanitarios públicos, investigación y formación en la ciudad de Barcelona a través de diferentes centros:

- Hospital del Mar
- Hospital de l'Esperanza
- Centre Fòrum de l'Hospital del Mar
- Centros Asistenciales Emili Mira (CAEM).
- Centros asistenciales:
    - Centre Peracamps
    - CSMIJ Ciutat Vella (Astilleros)
    - CSMIJ Sant Martí como Ramon Turro
    - CSMA – CSMIJ La Mina
    - CSMA San Martín Norte (Clot)
    - CSMA Martí i Julià (C/Irlanda Sta. Coloma de Gramenet)
    - HDIA Infanto Juvenil (Rec Comptal)

El Consorci también dispone de unas oficinas administrativas y centros de formación en un edificio de la Estación de Francia.

Los componentes básicos de la red objeto del servicio solicitado son los siguientes:

- Capa de acceso.
- Red Wi-Fi corporativa y red Wi-Fi para visitantes y pacientes.
- Capa de agregación – equipos de Core.
- Conmutación del Centro de Datos.
- Equipos de protección perimetral y cortafuegos.

La red LAN soporta principalmente los siguientes servicios:

- Servicio de telefonía corporativa sobre plataforma NEC.

- Datos corporativos. Informática de gestión. Estación de trabajo médica (ETM) y Estación de trabajo de enfermería (ETI).
- Integración de equipamiento de electromedicina (diagnóstico por la imagen, ecografías, radiología, ultrasonidos, etc.).
- Sistemas de telemetría y telecontrol de gestión de los edificios.
- Video-seguridad.
- Video-retransmisión de intervenciones quirúrgicas.
- Tele formación.
- Acceso a Internet corporativo.
- Acceso a Internet para visitas y pacientes.
- IP-TV, distribución de señales de televisión, actualmente en la UCI, pero ampliable a otros departamentos.
- Control de acceso y control horario.

Resumidamente, el alcance del servicio solicitado comprende:

- Inventario y estudio de la situación de la red LAN del CMPSB, previo a la prestación propiamente dicha del servicio solicitado.
- Mantenimiento preventivo y correctivo de los equipos de red LAN (Cisco) y protección perimetral (Paloalto), cortafuegos.
- Monitorización en remoto del estado de los equipos y su rendimiento, tanto de la red LAN como de la red WAN de interconexión entre los diferentes centros.
- Actualización de versiones de software de los equipos.
- Copias de seguridad de la configuración de los equipos.
- Emisión de informes regulares de rendimiento y explotación de la red.
- Servicio de consultas Help Desk.
- Apoyo en las tareas de administración de la red para tareas de cambios de configuración (move & change).
- Asesoramiento sobre la evolución de la red, discontinuidad de soporte de equipos, etc.
- Ampliaciones puntuales de la red, si es necesario.

La presente especificación técnica establece el alcance del servicio de mantenimiento y de apoyo a la administración que necesita el CMPSB. Define los requisitos técnicos y funcionales que deben cumplir el servicio y el proceso de migración de la situación actual a la nueva, afectando mínimamente a la operativa del hospital y minimizando el riesgo de indisponimlidad.

1.2. Modelo de explotación de la red

El modelo de gestión y explotación de la red LAN del CMPSB se ha definido en cuatro niveles:

I. Dirección: El responsable de la gestión de la red y de tomar todas las decisiones respecto a su explotación, diseño y configuración es el departamento de Sistemas de Información del CMPSB (SSI). El CMPSB nombrará un administrador de la red.

II. Administración: La administración diaria y regular de la red será asumida por el departamento de Sistemas de Información del CMPSB. El proveedor deberá asumir las siguientes tareas:

a. Monitorización en remoto con su propia plataforma de todos los equipos de la red.
b. Emisión proactiva de alarmas por avería o caída de rendimiento de elementos clave de la red todos los días las 24 horas del día.
c. Emisión regular de informes de explotación y rendimiento.
d. Emisión anual de un informe de explotación con recomendaciones y avisos de discontinuidad de equipos.
e. Realizar regularmente y mantener a resguardo copias de seguridad de las configuraciones de todos los equipos.
f. Actualización de las versiones de software de todos los equipos.

A petición expresa de los responsables del CMPSB, el proveedor deberá prestar también de manera puntual los siguientes servicios:

g. Apoyo Servicio de Atención
h. Cambios de configuración en remoto o de forma presencial de cualquier equipo.

III. Mantenimiento: Mantener en perfectas condiciones de funcionamiento todos y cada uno de los componentes de la red. El objetivo es garantizar la reposición del servicio en caso de avería lo antes posible. Se contemplan dos tipos:

a. Preventivo: Acciones destinadas a minimizar las probabilidades de que se produzca una incidencia que provoque la caída total de un equipo o afecte gravemente a su rendimiento.
b. Correctivo: Acciones destinadas a reponer lo más rápidamente posible las incidencias que afecten al correcto funcionamiento de la red y/o afecten gravemente a su rendimiento.

IV. Ampliaciones de la red: A petición del CMPSB, el proveedor deberá instalar y/o configurar nuevos equipos de red y protección perimetral y de CPD (Firewall interno y NAC), teniendo en cuenta que:

a. Hay previsión de cambio de los 2 firewalls perimetrales por 2 nuevos, que deberá incluir la instalación del equipamiento, y la migración y mejora de la aplicación de reglas actuales al nuevo equipamiento.
b. Hay previsión de adquisición de 2 firewalls de CPD (firewalls internos), que deberán instalarse y sobre los que se deberán aplicar las políticas de seguridad adecuadas para mejorar la segmentación y seguridad de toda red interna. Habrá que ejecutar una buena planificación de segmentación de red.
c. Hay previsión de adquisición de un NAC para 1000 dispositivos, sobre los que se deberán aplicar políticas de acceso con instalación del agente. Definir las políticas adecuadas para los dispositivos con el fin de mejorar la seguridad de la red.
d. Con todo este nuevo equipamiento de seguridad de firewalls perimetrales, firewalls internos de CPD y accesos NAC por 1000 dispositivos, se deberá mantener y mejorar las reglas necesarias para cumplir una mejor segmentación de la red interna y poder aislar equipamiento en el caso de que sea necesario a petición del CMPSB, el proveedor deberá suministrar, instalar y configurar nuevos equipos de red y protección perimetral.
e. Hay previsión de adquisición de 40 Switchs Cisco Meraki, que deberán instalarse físicamente en los diferentes rack's y configurarlos dentro de la red del hospital.

f. Hay previsión de adquisición de 60 Antenas Wi.Fi Cisco Meraki, que deberán configurarse dentro de la red del hospital.
g. Disponemos de 40 Switchs Cisco Meraki en stock, que deberán instalarse físicamente en los diferentes racks y configurarlos dentro de la red del hospital. Estos equipos están destinados para la sustitución del parque de switchs Cisco Catalyst aún instalados.

1.3. Requisitos y criterios generales

El CMPSB precisa que los potenciales proveedores cumplan obligatoriamente los siguientes requisitos mínimos:

- Dispongan de un centro de telecontrol, recepción y emisión de alarmas operativo todos los días del año y las 24 horas del día, y que atienda en castellano y/o catalán.
- Que disponga de un equipo de al menos 5 técnicos cualificados con amplia y demostrable experiencia en networking y ciberseguridad con sede operativa en el área metropolitana de Barcelona, ya que si no es imposible cumplir los tiempos de reposición del servicio establecido.
- Aporten un gestor de servicio con sede en el área metropolitana de Barcelona.
- Que tenga capacidad para facilitar un servicio de mantenimiento 24x7x4 sobre los equipos instalados en centros con este horario.

1.4. Calendario de implantación y duración del servicio.

El adjudicatario será responsable del servicio de mantenimiento y apoyo a la administración desde la formalización del contrato.

El adjudicatario asumirá el servicio de mantenimiento correctivo de la red antes de 15 días naturales a partir de la formalización del contrato.

Dispondrá de un plazo de 3 meses a partir de la formalización del contrato para activar la totalidad de los servicios solicitados.

El calendario del proceso de migración será acordado con el CMPSB.

El servicio se considerará operativo cuando se hayan llevado a cabo las siguientes tareas:

- Estudio de situación y documentación as-built de la red.
- Plataforma de gestión completamente configurada, incluyendo visibilidad y alarmas de la red de datos WAN. Consola operativa en el departamento de informática del CMPSB.
- Copias de seguridad de todos los equipos.
- Actualizaciones de software efectuadas.

El CMPSB efectuará pruebas de aceptación del servicio y todas las pruebas que considere oportunas por sí mismo o con apoyo de los asesores externos que estime oportuno antes de dar por iniciado propiamente el servicio.

La duración prevista del contrato será de 3 años a partir de la formalización del contrato, prevista para el 4 de diciembre de 2024, con posibilidad de prorrogarlo hasta un máximo de 2 años más.

El proveedor deberá comunicar al CMPSB si incumple en algún momento, a lo largo de la duración del contrato, alguno de los requisitos y si se trata de un incumplimiento circunstancial y puntual o no. En caso de que se incumplan los requisitos mínimos obligatorios establecidos de medios disponibles o de niveles de SLA, el CMPSB podrá rescindir el contrato unilateralmente y sin obligación de compensar al proveedor.

2. Descripción de la red

El CMPSB facilitará la descripción de la red de los diferentes centros durante la visita obligatoria prevista en el punto 17 de la memoria justificativa de esta licitación.

3. Servicio de mantenimiento

3.1. Definiciones preliminares:

- **Mantenimiento preventivo:** Acciones destinadas a minimizar las probabilidades de que se produzca o a evitar (prevenir) una incidencia que provoque una avería en un equipo o afecte gravemente a su rendimiento.
- **Mantenimiento correctivo:** Acciones destinadas a restablecer el nivel de servicio perdido lo más rápidamente posible debido a incidencias que afecten al correcto funcionamiento de la red y/o afecten gravemente a su rendimiento.
- **Tiempo de respuesta:** Es el periodo de tiempo que transcurre desde que se detecta o se comunica una avería o incidencia hasta que se inician las acciones destinadas a restablecer el nivel de servicio perdido con la incidencia.
- **Tiempo de reposición:** Es el período de tiempo que transcurre desde que se detecta o se comunica una avería hasta que queda restablecido el nivel de servicio perdido.
- **Cobertura:** Periodo de tiempo durante el cual están disponibles los recursos necesarios para realizar un servicio de mantenimiento, administración o Help Desk.

3.2. Plataforma de monitorización

El proveedor dispondrá de una plataforma de monitorización remota a la que incorporará todos los equipos de la red del CMPSB, incluidos los cortafuegos, y en modo lectura los equipos de la red WAN.

El CMPSB facilitará los contactos con los responsables del operador de telefonía que tiene actualmente contratado el servicio con el CMPSB.
En un futuro y durante la duración del servicio, el actual operador de telefonía podría ser sustituido por otro operador o por un gestor de soluciones SD-WAN.

Esta plataforma estará operativa permanentemente y con una disponibilidad mínima del 99,95%.

Debe cumplirse estrictamente con la normativa europea de gestión de datos de carácter personal. La información entre la red y el centro de control se transmitirá encriptada.

La conexión entre el centro de control y la red se hará bien a través de Internet, por lo que se configurarán adecuadamente los cortafuegos, o bien mediante un enlace dedicado MPLS o el que considere adecuado el proveedor asumiendo el coste del mismo.

La comunicación a través de redes públicas, Internet, se hará convenientemente protegida y encriptada, mediante soluciones VPN, tunelización, etc.

También se dispondrá de una conexión de reserva (back-up) para los casos de pérdida de conexión debido a caída del enlace o avería grave en los cortafuegos. El proveedor asumirá el coste de la línea de back-up.

Se instalará una consola de la plataforma de monitorización en el departamento de sistemas del CMPSB, ubicado en la estación de Francia. Se indicará si esta consola es autónoma, es decir, es operativa incluso en caso de pérdida de conexión con el Centro de Control del proveedor o no. El proveedor facilitará todo el equipo que sea necesario.

El idioma de la plataforma será inglés, castellano o catalán.

En la misma se programarán la emisión automática de alarmas críticas, generadas tanto por avería hardware, por pérdida de alimentación eléctrica y por superación de límites de tráfico soportado o rendimiento de equipo o empleo de memoria (thresholds o umbrales de alarma).

El proveedor, de acuerdo con el CMPSB, determinará cuáles son estas alarmas durante la fase de migración. Como mínimo se deberán contemplar las siguientes:

- Alertas sobre la pérdida de alimentación.
- Alertas sobre caídas del sistema de ventilación en equipos de agregación, core y cortafuegos.
- Avería en elementos clave, procesadores, memoria, etc. de los equipos de agregación, core y cortafuegos y conmutadores de quirófanos y unidades de vigilancia o cuidados intensivos.
- Caída de enlaces de red WAN.
- Thresholds, alarmas por superación de niveles de tráfico en determinados enlaces y/o por tipo de protocolo.
- Thresholds, alarmas por superación de niveles de rendimiento u ocupación de elementos críticos como procesadores y memorias.
- Detección de intrusiones y ataques.
- Alertas relacionadas con los firewalls de CPD

Las alarmas muy críticas se remitirán a los responsables del CMPSB por correo electrónico y/o a una app del smartphone.

Se calcula que habrá alrededor de 50 alarmas que deben tratarse como muy críticas. En cualquier caso, el proveedor propondrá una lista de alarmas críticas.

Se desea que el proveedor actúe de manera proactiva detectando la avería o alerta antes que el CMPSB en al menos un 75% de las ocasiones.

Se informa que actualmente el CMPSB dispone y utiliza la versión gratuita de la plataforma de gestión de infraestructuras tecnológicas Nagios y sus técnicos están formados y experimentados en el uso de esta plataforma. La plataforma propuesta por el proveedor debe integrarse y sincronizarse con la plataforma Nagios.

A pesar de lo indicado anteriormente, el CMPSB desea disponer del máximo de prestaciones y herramientas de gestión.

El proveedor indicará claramente qué plataforma utilizará y qué prestaciones ofrece. Entre otras cosas, se desea que permita como mínimo:

- Hacer de manera automática el mapa topológico de la red. Capacidad de "descubrir" la red.
- Detectar la conexión de nuevos equipos de red.
- Actualización automática para la corrección de errores, actualizaciones de seguridad y nuevas características.
- Herramientas de análisis de tráfico en tiempo real, como la captura de paquetes y la prueba de cables para aislar y solucionar problemas de red. Si es necesario el proveedor instalará las sondas necesarias para comprobar posibles problemas de lentitud, STP y otros problemas de red.
- Registro, logs, de los cambios de configuración de los equipos.
- En los equipos "zero touch provisioning", auto-despliegue, auto-configuración. En caso de sustitución, se podrá configurar automáticamente la recarga de la configuración sin intervención del operador. Indicar qué equipos instalados permiten esta prestación.
- Perfilado de dispositivos, es decir, reconocimiento del tipo de dispositivo y su sistema operativo, y disponer de la posibilidad de aplicar políticas basadas en dispositivo y/o sistema operativo.

3.3. Mantenimiento preventivo.

Con una periodicidad trimestral se llevará a cabo una visita a todos los racks y centros de datos del CMPSB que, como mínimo, contemplará los siguientes aspectos:

- Proceder a limpiar con aire a presión todos los ventiladores y sistemas de refrigeración de los equipos.
- Comprobar la limpieza de los nodos.
- Verificar que no se han efectuado cambios físicos ni ha habido intentos de manipulación de los equipos.
- Comprobar que los cables de conexión, cables de conexión cortos, etc., están bien ordenados e identificados correctamente.
- Comprobar que los protocolos de acceso y seguridad físico se aplican correctamente.
- Se fotografiarán todos los nodos y se remitirán al CMPSB estas fotografías que también se incorporarán a los informes correspondientes.

El proveedor presentará su propia propuesta de tareas de mantenimiento preventivo que incluya como mínimo los puntos indicados anteriormente.

3.4. Mantenimiento correctivo

El servicio de mantenimiento se llevará a cabo de acuerdo con los siguientes parámetros:

- Periodo de cobertura: según el horario de cada centro, indicado en el Annex I de este PPT.
- Electrónica de acceso: tiempo de reposición del servicio de 4 horas dentro del periodo de cobertura de cada centro.
- Red Wi-Fi: tiempo de reposición del servicio de 4 horas dentro del período de cobertura de cada centro.
- Electrónica de agregación: 24x7x4. Periodo de cobertura: todos los días del año. Tiempo máximo de reposición del servicio: 4 horas.
- Electrónica de DataCenter: 24x7x4. Periodo de cobertura: todos los días del año. Tiempo máximo de reposición del servicio: 4 horas.
- Cortafuegos perimetrales y de CPD: 24x7x4. Periodo de cobertura: todos los días del año. Tiempo máximo de reposición del servicio: 4 horas.

El mantenimiento correctivo, debido a avería hardware, incluye el reemplazo de equipos, tarjetas u otros componentes averiados por elementos iguales o compatibles de mayores prestaciones.

El objetivo es que se reponga el servicio con las mismas o superiores prestaciones a las que se disfrutaba antes de la incidencia o avería, aunque no se utilice un equipo del mismo modelo, siempre del propio fabricante.

4. Servicio apoyo a la administración

4.1. Servicio de ayuda

El proveedor, como parte del servicio que debe prestar, pondrá a disposición del CMPSB un servicio de soporte telefónico o Help Desk para la resolución de dudas o prestar apoyo a los administradores de la red. El servicio se prestará en catalán y/o castellano, los días laborables de 8 a 17 h., como mínimo.

4.2. Apoyo a la administración

El proveedor, como parte del servicio que debe prestar, pondrá a disposición del CMPSB un equipo de técnicos cualificados para apoyo en la administración de la red, altas, bajas, modificaciones, etc., de forma remota o presencial. El servicio se prestará en catalán y/o castellano.

Las solicitudes de apoyo que se puedan prestar remotamente se atenderán en un máximo de 12 horas de lunes a viernes de 8 a 21 horas.

Las actuaciones que requieran presencia física en los centros del CMPSB se atenderán en un máximo de dos días laborables.

4.3. Copias de seguridad

Dentro del plan de migración se harán copias de seguridad de la configuración de todos los equipos de la red. Las copias se guardarán en dos ubicaciones diferentes: en el servidor del CMPSB asignado, ubicado en el centro de datos principal, y en un servidor del proveedor.

Se configurarán los equipos de manera que automáticamente, cada vez que se haga una modificación, se actualice la copia de seguridad del equipo a las dos ubicaciones previstas.

Si no es posible la copia 100% automática, se establecerá un procedimiento de actuación para actualizar todas las copias de forma regular. La periodicidad con que se harán las copias dependerá de la periodicidad con que se hacen los cambios.

También se hará regularmente una copia de seguridad de la configuración de la plataforma de monitorización, de los niveles de alarma establecidos, del tipo de informes que se emiten, etc. Esta copia también se hará en un servidor del CMPSB y otro del proveedor.

4.4. Gestión de versiones

El proveedor será responsable de mantener todos los equipos actualizados y de cargar todas las actualizaciones de software, parches, etc.

En cuanto a los cortafuegos, también será el encargado de mantener todos los patrones y políticas de seguridad actualizadas.

Todas estas actualizaciones se harán de forma programada y con la previa autorización del administrador de la red.

4.5. Apoyo frente a ataques externos e instrucciones

En cuanto a la ciberseguridad, el proveedor deberá responsabilizarse de detectar ataques e intentos de intrusión en la red de cualquier origen, entre otros:

- A través de la conexión a Internet.
- A través de conexiones Wi-Fi del servicio Hot-spot público o intentos de conexión de dispositivos no autorizados al Wi-Fi corporativo.
- Por conexión de algún dispositivo no autorizado a alguna toma del sistema de cableado.

El proveedor debe justificar que dispone de recursos adecuados para hacer frente a estas incidencias.

4.6. Informe de gestión y estadísticas de uso

La empresa gestora elaborará mensualmente un informe de gestión que debe incluir como mínimo la siguiente información:

- Número de actuaciones de mantenimiento realizadas clasificadas por tipo.
- Informe de resolución de las incidencias muy graves, causas y actuaciones hechas y recomendaciones para que no se reproduzca la incidencia.
- Número de actuaciones de administración realizadas: Altas, Bajas, Modificaciones, etc., y el tiempo dedicado a las mismas.
- Estadísticas de tráfico de los segmentos Ethernet o enlaces críticos.

- Estadísticas de tráfico de los enlaces críticos de la WAN: ocupación máxima, mínima y media de cada segmento medidos en periodos de 5 minutos.
- Estadísticas de tráfico de la conexión a Internet: ocupación máxima, mínima y media de cada segmento medidos en periodos de 5 minutos.
- Rendimiento de los principales equipos: conmutadores core, conmutadores de data center, cortafuegos y conmutadores de acceso muy críticos, como quirófanos y UVI. (Ex. Switch)

El informe será emitido de forma electrónica, en PDF o Microsoft Office.

El proveedor indicará en su oferta el índice de este documento que emitirá mensualmente y que deberá incluir al menos los aproximadamente 50 parámetros o alarmas críticas estimadas.

Este informe se emitirá dentro de los 10 primeros días del mes siguiente.

4.7. Informe de explotación

Anualmente, se emitirá un informe de explotación con al menos el siguiente contenido:

- Resumen de las actuaciones efectuadas tanto de mantenimiento como de apoyo a la administración.
- Resumen de las estadísticas de uso emitidas. Gráficas de evolución de los elementos o parámetros críticos.
- Propuesta de mejora y recomendaciones de inversión convenientemente justificadas.
- Avisos relativos a la vida de los equipos y el soporte que ofrece el fabricante y el que ofrece el proveedor.
- Nivel de cumplimiento SLA.

Este informe se emitirá antes de 30 días, finalizados los periodos anuales, que no tienen por qué coincidir con el año natural.

4.8. SOC Servicios Gestionados de Seguridad

Todos estos servicios deberán coordinarse y conciliarse con el servicio de Sistemas del CMPSB, asegurando una integración eficiente y fluida en los procesos existentes. Esta colaboración garantizará que cualquier intervención, actualización o resolución de incidentes se realice siguiendo los procedimientos establecidos por el servicio de Sistemas, manteniendo la coherencia con las políticas de seguridad, las infraestructuras tecnológicas y las operaciones diarias del CMPSB. Además, será esencial establecer una comunicación constante para asegurar que las actuaciones de los diferentes equipos no interfieran con las tareas críticas o comprometan la disponibilidad de los sistemas.

Servicios 24hX7d

- Vigilancia de infraestructuras

  - Supervisión permanente de los parámetros asociados al estado y la disponibilidad de las infraestructuras de seguridad.
  - Desencadenamiento de alertas ante situaciones anómalas o desviaciones respecto a los valores de referencia definidos, para la detección preventiva de sobrecargas y de elementos infrautilizados.
- Gestió d'Alertes (SIEM)
  - Recogida y almacenamiento del histórico de registros generados por los equipos de seguridad para su análisis posterior.
  - Correlación avanzada de eventos: Detección de ataques, vulnerabilidades, virus, accesos no autorizados, atacantes, equipos atacados, patrones de comportamiento... y las horas en que se producen, determinando la criticidad, relevancia y falsos positivos.
  - Análisis, filtrado y calificación de las alertas de seguridad detectadas en base a una escala de riesgo.
- Respuesta ante incidentes
  - Ejecución de procedimientos de comunicación, actuación y escalado.
  - Primer nivel de diagnóstico, mitigación y escalado por parte del Equipo de Respuesta ante Incidentes.
  - Mitigación experta o de segundo nivel ante incidentes de mayor complejidad (diagnóstico profundo e involucración de todo el personal de apoyo experto para la neutralización y recuperación total de los sistemas afectados).
  - Sistema de automatización de contramedidas para la contención y mitigación del impacto ante amenazas habituales o conocidas.
  - Registro de documentación y almacenamiento en BBDD de incidentes conocidos (amenazas, evidencias, procedimientos, medidas correctoras aplicadas para la resolución de los incidentes detectados, ...).

Mensual

- Gestión de informes
  - Informe de incidencias (desglose por clasificación, prioridad y tecnología), acumulado estadístico histórico y tendencias.
  - Inventario monitorizado (Nombre, modelo, IP, Número de serie, Versión de firmware, localización de chasis y tarjetas, altas y bajas).
  - Informe de incidentes y eventos de seguridad significativos (procedencia, criticidad, topología, ataques y falsos positivos/negativos).
  - Resto de capítulos dedicados a cada uno de los servicios incluidos.
  - Boletines de seguridad: Tendencias del mercado, nuevos ataques, posibles nuevas vulnerabilidades, etc.

- Cuadros de mando: Acceso remoto y seguro a un portal único y personalizado con la representación gráfica y lógica en tiempo real de parámetros críticos del servicio.

Servicios semestrales

- Gestión de Vulnerabilidades
  - Escaneo automático de equipos:
    - Análisis periódico de vulnerabilidades sobre equipos para detectar puertos abiertos y vulnerabilidades reportadas. Escaneo y análisis desde dentro y fuera de la subraya en estudio (intranet / extranet). Informe automático de recomendaciones técnicas y operativas para la resolución de las vulnerabilidades identificadas.
  - Servicio de alerta:
    - Recopilación, análisis y almacenamiento de informes de vulnerabilidades emitidos por los fabricantes. Explotación de sistemas de información compartida para la recogida de feeds relativos a malware, fuentes de reputación e incidentes de seguridad. Retroalimentación de BBDD de inteligencia contra amenazas de la plataforma SIEM para una mayor efectividad en la detección de amenazas.

4.9. Soporte gestión redes WiFi

El proveedor tendrá capacidad de prestar apoyo en la administración de la red Wi-Fi tanto:

- Acceso inalámbrico a la LAN interna del hospital para el personal sanitario.
- Acceso público a Internet para pacientes y visitas (servicio Hot-spot), que está actualmente gestionado desde la plataforma de meraki.

En cuanto al servicio Hot-spot, se deberá tener capacidad para apoyar en relación, entre otros, a los siguientes aspectos, tanto en la infraestructura Meraki como en la antigua:

- Garantizar que ambos servicios, público y corporativo, aunque comparten los mismos equipos, están completamente aislados a nivel lógico y el tráfico priorizado adecuadamente, siempre en detrimento del tráfico de hot-spot.
- Control de acceso de visitantes y pacientes mediante códigos de autorización temporal.
- Control de navegación, bloqueo de webs, etc. Filtrado de acceso a contenidos ilegales y otros que se determinen.
- Registro de navegación según la legislación vigente.

- Bloqueo/autorización de servicios, por ejemplo, streaming de vídeo, descargas de ficheros de grandes dimensiones, etc.
- Protección entre usuarios.
- Capacidad de asignar un caudal máximo total del servicio.
- Capacidad de asignar un caudal máximo por usuario.
- Pantalla de bienvenida al servicio y de aceptación de condiciones.
- Protección frente a intrusiones. Tener en cuenta que el Hospital del Mar se encuentra frente a la playa, en una zona con gran afluencia de público.
- Ajuste, preferentemente de forma automática, de todos los Access Points que componen la red, especialmente en los aspectos relativos a la radio, frecuencia, canales, etc. Establecer, de forma automática, la potencia de transmisión y el canal de cada Access Point.
- Detección automática de conexiones de antenas no autorizadas.
- Detección de interferencias con otras redes.
- Capacidad de crear mapas de cobertura.
- Monitorización del rendimiento del sistema, etc.
- Detección de intentos de intrusión.
- Autenticación mediante usuario y contraseña integrado con Active Directory.

Como parte del estudio de situación, se deberá comprobar el estado de todos los aspectos relacionados a continuación y solucionar las deficiencias detectadas y efectuar las recomendaciones de mejora oportunas.

El estudio de situación también contemplará la posible integración a efectos de gestión de las dos redes Wi-Fi.

Adicionalmente, el proveedor tendrá capacidad para dar soporte en el despliegue y administración sobre la red Wi-Fi de los siguientes servicios:

- Servicios de analítica de localización sin necesidad de licencias adicionales ni hardware adicional.
- Servicios de analítica de presencia de usuarios, que permita controlar los flujos de personas y la afluencia de público a las instalaciones y sus diferentes áreas.

5. Gobernación

El CMPSB desea establecer un entorno de colaboración eficaz con el proveedor que garantice un alto nivel de disponibilidad de la red, minimizando los riesgos de incidencias y adelantándose a los riesgos de obsolescencia y/o falta de capacidad.

Para ello, es imprescindible establecer una comunicación fluida y unos procedimientos de coordinación simples, claros, concretos y eficaces. Por tanto, el ofertante presentará, acompañando su oferta, una propuesta completa de gobernanza del servicio. Esta propuesta incluirá una relación de procedimientos de coordinación y su desarrollo. Entre otros, se desarrollarán los siguientes procedimientos:

- Gestión de incidencias:
  - En la red WAN.
  - LAN.
  - Para sobrepasar umbrales de tráfico o rendimiento de los equipos.
- Copias de seguridad.
- Actualizaciones de versiones de software.
- Apertura de incidencias de forma manual.
- Apoyo de administración.
- Acceso a Help Desk.
- Acceso a las instalaciones del CMPSB.

6. Contratos, garantías, y acuerdos de nivel de servicio

El objetivo de los servicios contratados a través de este pliego es que el CMPSB alcance un alto grado de disponibilidad de la red. Se desea alcanzar una disponibilidad global mínima del 99,5%, es decir, que la red esté completamente operativa durante todo el año, 24 horas al día, el 99,5% del tiempo.

Por lo tanto, el requerimiento de nivel de servicios SLA (del inglés Service Level Agreement) tendrá un horario de cobertura de 24x7 con un tiempo máximo de respuesta de 4 horas. Este acuerdo contemplará niveles de servicio global y para cada uno de los componentes del servicio:

Mantenimiento preventivo y correctivo:

- Capa de acceso
- Wifi corporativa
- Wifi pública
- Capa de agregación
- Centro de datos de Capa
- Cortafuegos
- Monitorización remota
- Servicio de ayuda
- Apoyo a la administración
- Copias de seguridad
- Emisión de informes:
- Estadísticas mensuales de uso
- Informe anual

El contrato propuesto contemplará penalizaciones por incumplimiento de los niveles de SLA y especificará los instrumentos de control de los mismos y todas las fórmulas de cálculo.

El incumplimiento reiterado de las SLA global o de dos correspondientes a otros componentes del servicio durante tres meses consecutivos o 6 alternos durante un año, habilitará al CMPSB a rescindir unilateralmente el servicio sin compensar al proveedor de ninguna manera.

El CMPSB valora los compromisos que se adquieren en este punto y las penalizaciones propuestas. (Punto 14.2.4 del PCA)

7. Plan de migración y activación del servicio

7.1. Dirección

El presente proyecto es responsabilidad de la Dirección de Sistemas de Información y comunicaciones del CMPSB, que nombrará a un administrador de la red como interlocutor principal con el proveedor.

7.2. Responsable del servicio

El adjudicatario nombrará un responsable del servicio, que será el interlocutor principal con el administrador de la red.

El responsable del servicio asistirá a las reuniones de seguimiento a que lo convoque el CMPSB, aproximadamente una por trimestre. Durante el primer semestre de operación del servicio, las reuniones tendrán una frecuencia superior, con un máximo de una al mes.

Asistirá a las reuniones de coordinación con otros posibles proveedores del departamento de sistemas a que se le convoque, especialmente con el proveedor de la WAN.

7.3. Equipo de trabajo

Se indicará la composición del grupo de trabajo, su experiencia, el organigrama, el perfil de los trabajadores que destinarán al servicio objeto del contrato y donde se demuestre que cumplen con los requisitos mínimos solicitados al PPT.

El equipo dispondrá de un mínimo de 8 técnicos con base en el área metropolitana de Barcelona. Se pide que la licitadora disponga de una base (oficina o taller) en el área metropolitana de Barcelona, aunque su central pueda estar ubicada en cualquier otra población. Esta solicitud se fundamenta en la necesidad de cumplir con el SLA establecido, que exige un tiempo máximo de resolución de 4 horas, dada la naturaleza crítica del servicio.

Se facilitará el historial profesional de todo el personal perteneciente al equipo de trabajo donde se indicará qué certificados de los fabricantes disponen y su fecha de obtención y caducidad.

El grupo de trabajo estará sujeto a la previa conformidad del CMPSB.

Los técnicos asignados al grupo de trabajo deberán contar con una experiencia acreditada mínima de dos años en el ámbito objeto de esta licitación. Esta experiencia se justificará mediante la presentación del Currículo Vitae correspondiente.

El grupo de trabajo deberá contar, en conjunto, con la formación certificada correspondiente, acreditada mediante las certificaciones oficiales de Cisco, Fortinet y Palo Alto.

Los certificados mínimos solicitados son los siguientes :

Cisco:

- CCNA.
- CCNP Empresa.
- Proveedor de servicios CCNP.
- Cisco Certified Specialist - Implementación de infraestructuras avanzadas empresariales.

- Especialista certificat de Cisco - Nucli empresarial.
- Especialista certificado de Cisco - Diseño empresarial.
- Cisco Certified Specialist - Implementación de encaminamiento avanzado del proveedor de servicios.
- Especialista certificado de Cisco - Núcleo de proveedor de servicios.
- Cisco Certified Specialist - Implementación de servicios VPN para proveedores de servicios.
- Responsable de éxito del cliente de Cisco.

Fortinet:

- Fortinet Certified Fundamentos en Ciberseguridad.
- Seguridad de red profesional certificada Fortinet.
- Especialista en soluciones certificadas Fortinet en seguridad de red.

Palo Alto:

- Ingeniero de seguridad de red certificado por Palo Alto Networks PCNSE
- Ingeniero de cortafuegos de software certificado por Palo Alto Networks PCSFE
- Ingeniero de sistemas acreditado por Palo Alto Networks - Software Firewall Professional
- Palo Alto Networks Ingeniero de Sistemas Profesional Strata
- PSE de Palo Alto Networks: SASE Profesional

7.4. Activación del servicio

El adjudicatario asumirá el servicio de mantenimiento correctivo de la red antes de 15 días naturales a partir de la formalización del contrato. Dispondrá de un plazo de 3 meses a partir de la formalización del contrato para activar la totalidad de los servicios previstos.

7.5. Plan de migración

El licitador deberá presentar una propuesta de plan de migración o lanzamiento del servicio, que describa el programa detallado de trabajo que estime más oportuno y que garantice que está preparado para asumir el mantenimiento y las tareas de apoyo a la administración de acuerdo con lo previsto en este pliego.

El proceso de migración debe contemplar obligatoriamente las siguientes tareas:

- Estudio de situación con el siguiente contenido mínimo:
    - Documentación AS-Built de la red.
    - La configuración de todos los equipos.
    - Diagramas de bloques.
    - Comprobación y documentación de la alimentación eléctrica de todos los equipos, incluyendo el tipo de protecciones eléctricas, magnetotérmicos y diferenciales.
    - Esquemas de conexión.
    - Funcionamiento de los hot-spots wifi.
    - Relación de recomendaciones de mejora para aumentar el rendimiento, la fiabilidad y la disponibilidad de la red.

- Activación del sistema de monitorización.
- Instalación de la consola del sistema de monitorización en las instalaciones del CMPSB e integración y sincronización con la plataforma Nagios.
- Instalación de la app en los teléfonos inteligentes del departamento de sistemas.
- Incorporación, a nivel de lectura, de los equipos de red WAN de la operadora de telefonía contratada por el CMPSB o quien pueda sustituirla en el futuro.
- Actualización de las versiones de software de los equipos.
- Copias de seguridad de la configuración de todos los equipos.
- Formación del personal de sistemas del CMPSB.
- Plan de migración para el traspaso del servicio a un nuevo proveedor una vez finalizado el periodo contratado.

La duración máxima del plan de migración se ha establecido en 10 semanas; todo el proceso desde la formalización del contrato debe estar finalizado antes de 3 meses.

El plan indicará:

- Una relación detallada de las etapas y actividades a realizar con el resultado a obtener en cada una de ellas, los recursos asignados y la documentación a emitir. El plan no debe provocar indisponibilidad de la red actual, ya que esta es crítica para la operativa del Hospital.
- Calendario detallado del proyecto.
- Pruebas de aceptación y procedimientos de control de calidad.
- Plan de seguridad y salud en el trabajo adaptado a los servicios que se prestarán, de acuerdo con los requisitos establecidos por la legislación vigente.

7.6. Colaboración leal

El presente servicio es una parte crítica de la operativa del CMPSB, en la que colaboran diferentes empresas. El licitador debe comprometerse a colaborar lealmente con estas empresas, aunque se trate de un competidor directo. Deberá colaborar especialmente con el operador de telefonía actual como proveedor de la red WAN o con el operador que lo pueda sustituir en el futuro.

El proveedor colaborará lealmente con la empresa que lo sustituya una vez finalizado el contrato, en caso de no resultar adjudicatario de la siguiente licitación.

7.7. Pruebas de aceptación

El CMPSB podrá realizar por sí misma o con apoyo externo las auditorías e inspecciones que considere oportunas antes de aceptar el inicio del servicio y durante su duración.

El ofertante presentará un plan detallado de Pruebas de aceptación que garanticen que presta el servicio conforme a lo previsto en las presentes especificaciones.

El proveedor, en presencia del CMPSB y eventualmente de los asesores que ésta considere oportunos, demostrará el perfecto funcionamiento de la plataforma de monitorización. El proveedor aportará, si es necesario, la instrumentación que se requiera para este fin, como elementos de generación de tráfico, etc.

Las pruebas de aceptación no deberán afectar al normal funcionamiento de la red.

A continuación, se relacionan los aspectos que obligatoriamente debe incorporar el plan de aceptación:

- Detección de la caída de un enlace.
- Detección de un intento de intrusión por el enlace de Internet.
- Detección de un ataque de DOS sobre los servidores públicos del CMPSB.
- Correcta configuración de los Sistemas de Gestión.
- Protección contra intrusión de la red Wi-Fi:
    - Entre usuarios del hot-spot o red pública.
    - De la red pública a la red interna del hospital.
- Comportamiento de los equipos ante la caída de un enlace.
- Cambio de ventiladores y fuentes de alimentación en caliente.
- Comportamiento en caso de corte de alimentación eléctrica.
- Simulación de altos niveles de tráfico superiores a los límites establecidos.
- Control de ancho de banda de la WAN y del enlace a Internet.
- Identificación de usuarios de hot-spot público.

Se firmarán las correspondientes actas de aceptación.

7.8. Documentación

El proveedor deberá entregar, una vez finalizado el estudio de situación y antes del inicio efectivo del servicio, la siguiente documentación:

- Estudio de situación.
- Manuales de uso de la plataforma de monitorización.
- Configuración de la plataforma de monitorización con los niveles de alarma determinados.
- Claves de usuario para acceder a la plataforma de manuales y documentación de los fabricantes.
- Documentación visual de la red de los diferentes centros y actualizada como mínimo cuatrimestralmente.

Se recuerda que a lo largo del servicio emitirá:

- Mensualmente el informe de gestión y estadísticas de uso.
- Anualmente el informe de explotación.

También se tramitará y facilitará el acceso a las plataformas de apoyo de los fabricantes, que incluyen:

- Resolución de casos.
- Manuales actualizados.
- Anuncios de nuevas versiones, etc.

8. Formación

El CMPSB desea que su departamento de sistemas, actualmente formado por 4 personas, reciba formación continuada en tecnologías y gestión de red. Por ello, dentro del servicio solicitado se incluirá:

1) Curso de formación inicial con el objetivo de:
    a) Capacitarlos en la utilización de la plataforma de monitorización remota y de su potencial. Incluyendo aspectos como:
        i) Detección y atención inmediata de las averías, aprendiendo a discriminar el elemento averiado o fuera de servicio y evaluar la importancia de la misma.
        ii) Utilización de la plataforma para que puedan programar y reconfigurar los equipos, extraer informes de utilización o tráfico, hacer seguimiento de las alarmas, realizar la reposición del sistema, ejecutar los programas de mantenimiento, etc.
        iii) Obtener estadísticas de tráfico, tanto puntuales, como regulares: disponibilidad, tráfico cursado y recibido por los diferentes enlaces, etc.
    b) Comprensión de los procedimientos de coordinación con el proveedor.

2) Curso anual de formación continua con el objetivo de:
    a) Conocer los últimos desarrollos y mejoras en tecnologías de networking IP y ciberseguridad.
    b) Conocer las prestaciones de las nuevas versiones de software de los equipos.

Se facilitará en la oferta una propuesta de contenido del curso de formación y de los certificados que se entregarán a los asistentes.

Hay que tener en cuenta que los técnicos del departamento de sistemas de información del CMPSB disponen de amplios conocimientos y una dilatada experiencia en gestión de redes Ethernet. Por ello, los cursos solicitados deben ser de nivel avanzado. En ningún caso se desea asistir a cursos básicos.

9. Ampliaciones puntuales

El CMPSB, con el objetivo de solucionar rápidamente problemas relacionados con el buen funcionamiento de la red, puede precisar que la empresa que presta el servicio de mantenimiento y apoyo a la administración tenga capacidad de suministrar e instalar equipos nuevos de la capa de acceso y antenas para ampliar la red inalámbrica WIFI.

El proveedor propondrá los siguientes equipos del mismo fabricante y compatibles con los actuales:

- Conmutador de 24 puertos.
- Conmutador de 48 puertos.
- Antena punto de acceso.
- Ampliación de equipos CPD.

El modelo y precio del equipo instalado se actualizará anualmente en función de la paridad €/$.

Estos equipos se incorporarán al servicio de mantenimiento y apoyo a la administración.

10. Presentación de ofertas

10.1. Sobre número 2

El proveedor deberá ofrecer un servicio que cumpla fielmente las condiciones y requerimientos citados en estas especificaciones.

Deberá facilitar toda la información necesaria para garantizar que está cualificado para prestar el servicio solicitado.

Se presentará la oferta en soporte informático estándar, Microsoft Office y AUTOCAD, o PDF, con la estructura que se describe en los siguientes apartados.

El contenido del sobre técnico será:

- Certificados del grupo de trabajo, detallados en el punto 7.3 de este documento.
- Compromiso de que se cumplen las especificaciones y se asumen los compromisos solicitados.

El sobre número 2 no incorporará ningún dato económico ni información sobre los certificados de los fabricantes.

Toda la oferta deberá ser clara, concreta y concisa, respondiendo a todos los puntos contemplados y en el orden expuesto anteriormente. Se valorarán con "0" cero puntos aquellas ofertas que no cumplan estrictamente estos requisitos.

10.2. Sobre número 3

Se deberá incluir la oferta económica, de conformidad con el modelo del Anexo 2 del PCAP, y los certificados de los fabricantes valorables de acuerdo con el punto 14.1.2 de los Criterios evaluables de forma automática incluidos en el Annex 4 del PCAP.

Barcelona, en la fecha de firma electrónica

Pablo Andolz Cardó
Jefe de Sistemas del CMPSB