PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL SERVEI DE MANTENIMENT I ADMINISTRACIÓ DE LES XARXES DE DADES DEL CONSORCI MAR PARC DE SALUT DE BARCELONA

1. Objectiu

1.1. Introducció

L'objecte del contracte correspon a la realització del servei de manteniment i administració de les xarxes de dades dels Centres del Consorci Mar Parc de Salut de Barcelona.

El Consorci Mar Parc de Salut de Barcelona (CMPSB) ofereix serveis sanitaris públics, recerca i formació a la ciutat de Barcelona a través de diferents centres:

- Hospital del Mar
- Hospital de l'Esperança
- Centre Fòrum de l'Hospital del Mar
- Centres Assistencials Emili Mira (CAEM).
- Centres assistencials:
    - Centre Peracamps
    - CSMIJ Ciutat Vella (Drassanes)
    - CSMIJ Sant Martí (Ramon Turró)
    - CSMA – CSMIJ La Mina
    - CSMA San Martí Nord (Clot)
    - CSMA Martí i Julià (C/Irlanda Sta. Coloma de Gramenet)
    - HDIA Infanto Juvenil (Rec Comptal)

El Consorci també disposa d'unes oficines administratives i centres de formació en un edifici de l'Estació de França.

Els components bàsics de la xarxa objecte del servei sol·licitat són els següents:

- Capa d'accés.
- Xarxa Wi-Fi corporativa i xarxa Wi-Fi per a visitants i pacients.
- Capa d'agregació – equips de Core.
- Commutació del Centre de Dades.
- Equips de protecció perimetral i tallafocs.

La xarxa LAN suporta principalment els serveis següents:

- Servei de telefonia corporativa sobre plataforma NEC.
- Dades corporatives. Informàtica de gestió. Estació de treball mèdica (ETM) i Estació de treball d'infermeria (ETI).

- Integració d'equipament d'electromedicina (diagnòstic per la imatge, ecografies, radiologia, ultrasons, etc.).
- Sistemes de telemetria i telecontrol de gestió dels edificis.
- Video-seguretat.
- Video-retransmissió d'intervencions quirúrgiques.
- Tele formació.
- Accés a Internet corporatiu.
- Accés a Internet per a visites i pacients.
- IP-TV, distribució de senyals de televisió, actualment a la UCI, però ampliable a altres departaments.
- Control d'accés i control horari.

Resumidament, l'abast del servei sol·licitat comprèn:

- Inventari i estudi de la situació de la xarxa LAN del CMPSB, previ a la prestació pròpiament dita del servei sol·licitat.
- Manteniment preventiu i correctiu dels equips de xarxa LAN (Cisco) i protecció perimetral (Paloalto), tallafocs.
- Monitorització en remot de l'estat dels equips i el seu rendiment, tant de la xarxa LAN com de la xarxa WAN d'interconnexió entre els diferents centres.
- Actualització de versions de programari dels equips.
- Còpies de seguretat de la configuració dels equips.
- Emissió d'informes regulars de rendiment i explotació de la xarxa.
- Servei de consultes Help Desk.
- Suport en les tasques d'administració de la xarxa per a tasques de canvis de configuració (move & change).
- Assessorament sobre l'evolució de la xarxa, discontinuïtat de suport d'equips, etc.
- Ampliacions puntuals de la xarxa, si cal.

La present especificació tècnica estableix l'abast del servei de manteniment i de suport a l'administració que necessita el CMPSB. Defineix els requisits tècnics i funcionals que han de complir el servei i el procés de migració de la situació actual a la nova, afectant mínimament l'operativa de l'hospital i minimitzant el risc d'indisponiblitat.

1.2. Model d'explotació de la xarxa

El model de gestió i explotació de la xarxa LAN del CMPSB s'ha definit en quatre nivells:

I. Direcció: El responsable de la gestió de la xarxa i de prendre totes les decisions respecte a la seva explotació, disseny i configuració és el departament de Sistemes d'Informació del CMPSB (SSI). El CMPSB nomenarà un administrador de la xarxa.

II. Administració: L'administració diària i regular de la xarxa serà assumida pel departament de Sistemes d'Informació del CMPSB. El proveïdor haurà d'assumir les següents tasques:

a. Monitorització en remot amb la seva pròpia plataforma de tots els equips de la xarxa.
b. Emissió proactiva d'alarmes per avaria o caiguda de rendiment d'elements clau de la xarxa tots els dies les 24 hores del dia.
c. Emissió regular d'informes d'explotació i rendiment.
d. Emissió anual d'un informe d'explotació amb recomanacions i avisos de discontinuïtat d'equips.
e. Realitzar regularment i mantenir a resguard còpies de seguretat de les configuracions de tots els equips.
f. Actualització de les versions de programari de tots els equips.

A petició expressa dels responsables del CMPSB, el proveïdor haurà de prestar també de manera puntual els següents serveis:

g. Suport Help Desk
h. Canvis de configuració en remot o de forma presencial de qualsevol equip.

III. Manteniment: Mantenir en perfectes condicions de funcionament tots i cadascun dels components de la xarxa. L'objectiu és garantir la reposició del servei en cas d'avaria el més aviat possible. Es contemplen dos tipus:

a. Preventiu: Accions destinades a minimitzar les probabilitats que es produeixi una incidència que provoqui la caiguda total d'un equip o afecti greument al seu rendiment.
b. Correctiu: Accions destinades a reposar el més ràpidament possible les incidències que afectin al correcte funcionament de la xarxa i/o afectin greument al seu rendiment.

IV. Ampliacions de la xarxa: A petició del CMPSB, el proveïdor haurà d'instal·lar i/o configurar nous equips de xarxa i protecció perimetral i de CPD (Firewall intern i NAC), tenint en compte que:

a. Hi ha previsió de canvi dels 2 firewalls perimetrals per 2 nous, que haurà d'incloure la instal·lació del equipament, i la migració i millora de l'aplicació de regles actuals al nou equipament.
b. Hi ha previsió d'adquisició de 2 firewalls de CPD (firewalls interns), que s'hauran d'instal·lar i sobre els que s'hauran d'aplicar les polítiques de seguretat adients per millorar la segmentació i seguretat de tota xarxa interna. Caldrà executar una bona planificació de segmentació de xarxa.
c. Hi ha previsió d'adquisició d'un NAC per a 1000 dispositius, sobre els que s'hauran d'aplicar polítiques d'accés amb instal·lació de l'agent. Definir les polítiques adients pels dispositius per tal de millorar la seguretat de la xarxa.
d. Amb tot aquest nou equipament de seguretat de firewalls perimetrals, firewalls interns de CPD y accessos NAC per 1000 dispositius, s'haurà de mantenir i millorar les regles necessàries per tal de complir una millor segmentació de la xarxa interna i poder aïllar equipament en el cas que sigui necessari a petició del CMPSB, el proveïdor haurà de subministrar, instal·lar i configurar nous equips de xarxa i protecció perimetral.
e. Hi ha previsió d'adquisició de 40 Switchs Cisco Meraki, que s'hauran d'instal·lar físicament als diferents rack's i configurar-los dins de la xarxa de l'hospital.
f. Hi ha previsió d'adquisició de 60 Antenes Wi.Fi Cisco Meraki, que s'hauran de configurar dins de la xarxa de l'hospital.
g. Disposem de 40 Switchs Cisco Meraki en estoc, que s'hauran d'instal·lar físicament als diferents racks i configurar-los dins de la xarxa de l'hospital.

Aquests equips estan destinats per la substitució del parc de switchs Cisco Catalyst encara instal·lats.

1.3. Requisits i criteris generals

El CMPSB precisa que els potencials proveïdors compleixin obligatòriament els següents requisits mínims:

- Disposin d'un centre de telecontrol, recepció i emissió d'alarmes operatiu tots els dies de l'any i les 24 hores del dia, i que atengui en castellà i/o català.
- Que disposi d'un equip d'almenys 5 tècnics qualificats amb àmplia i demostrable experiència en networking i ciberseguretat amb seu operativa a l'àrea metropolitana de Barcelona, ja que si no és impossible complir els temps de reposició del servei establert.
- Aportin un gestor de servei amb seu a l'àrea metropolitana de Barcelona.
- Que tingui capacitat per facilitar un servei de manteniment 24x7x4 sobre els equips instal·lats en centres amb aquest horari.

1.4. Calendari d'implantació i durada del servei.

L'adjudicatari serà responsable del servei de manteniment i suport a l'administració des de la formalització del contracte.

L'adjudicatari assumirà el servei de manteniment correctiu de la xarxa abans de 15 dies naturals a partir de la formalització del contracte.

Disposarà d'un termini de 3 mesos a partir de la formalització del contracte per activar la totalitat dels serveis sol·licitats.

El calendari del procés de migració serà acordat amb el CMPSB.

El servei es considerarà operatiu quan s'hagin dut a terme les següents tasques:

- Estudi de situació i documentació as-built de la xarxa.
- Plataforma de gestió completament configurada, incloent visibilitat i alarmes de la xarxa de dades WAN. Consola operativa al departament d'informàtica del CMPSB.
- Còpies de seguretat de tots els equips.
- Actualitzacions de programari efectuades.

El CMPSB efectuarà proves d'acceptació del servei i totes les proves que consideri oportunes per si mateix o amb suport dels assessors externs que estimi oportú abans de donar per iniciat pròpiament el servei.

La durada prevista del contracte serà de 3 anys a partir de la formalització del contracte, prevista per al 4 de desembre de 2024, amb possibilitat de prorrogar-ho fins a un màxim de 2 anys més.

El proveïdor haurà de comunicar al CMPSB si incompleix en algun moment, al llarg de la durada del contracte, algun dels requisits i si es tracta d'un incompliment circumstancial i puntual o no.

En cas que s'incompleixin els requisits mínims obligatoris establerts de mitjans disponibles o de nivells de SLA, el CMPSB podrà rescindir el contracte unilateralment i sense obligació de compensar al proveïdor.

2. Descripció de la xarxa

El CMPSB facilitarà la descripció de la xarxa dels diferents centres durant la visita obligatòria prevista al punt 17 de la memòria justificativa d'aquesta licitació.

3. Servei de manteniment

3.1. Definicions preliminars:

- **Manteniment preventiu:** Accions destinades a minimitzar les probabilitats que es produeixi o a evitar (prevenir) una incidència que provoqui una avaria en un equip o afecti greument al seu rendiment.
- **Manteniment correctiu:** Accions destinades a restablir el nivell de servei perdut el més ràpidament possible a causa d'incidències que afectin al correcte funcionament de la xarxa i/o afectin greument al seu rendiment.
- **Temps de resposta:** És el període de temps que transcorre des que es detecta o es comunica una avaria o incidència fins que s'inicien les accions destinades a restablir el nivell de servei perdut amb la incidència.
- **Temps de reposició:** És el període de temps que transcorre des que es detecta o es comunica una avaria fins que queda restablert el nivell de servei perdut.
- **Cobertura:** Període de temps durant el qual estan disponibles els recursos necessaris per realitzar un servei de manteniment, administració o Help Desk.

3.2. Plataforma de monitorització

El proveïdor disposarà d'una plataforma de monitorització remota a la qual incorporarà tots els equips de la xarxa del CMPSB, inclosos els tallafocs, i en mode lectura els equips de la xarxa WAN.

El CMPSB facilitarà els contactes amb els responsables de l'operador de telefonia que té actualment contractat el servei amb el CMPSB.
En un futur i durant la durada del servei, l'actual operador de telefonia podria ser substituït per un altre operador o per un gestor de solucions SD-WAN.

Aquesta plataforma estarà operativa permanentment i amb una disponibilitat mínima del 99,95%.

S'ha de complir estrictament amb la normativa europea de gestió de dades de caràcter personal.
La informació entre la xarxa i el centre de control es transmetrà encriptada.
La connexió entre el centre de control i la xarxa es farà bé a través d'Internet, per la qual cosa es configuraran adequadament els tallafocs, o bé mitjançant un enllaç dedicat MPLS o el que consideri adequat el proveïdor assumint el cost d'aquest.

La comunicació a través de xarxes públiques, Internet, es farà convenientment protegida i encriptada, mitjançant solucions VPN, tunelització, etc.

També es disposarà d'una connexió de reserva (back-up) per als casos de pèrdua de connexió a causa de caiguda de l'enllaç o avaria greu en els tallafocs. El proveïdor assumirà el cost de la línia de back-up.

S'instal·larà una consola de la plataforma de monitorització al departament de sistemes del CMPSB, ubicat a l'estació de França. S'indicarà si aquesta consola és autònoma, és a dir, és operativa fins i tot en cas de pèrdua de connexió amb el Centre de Control del proveïdor o no. El proveïdor facilitarà tot l'equip que sigui necessari.

L'idioma de la plataforma serà anglès, castellà o català.

En la mateixa es programaran l'emissió automàtica d'alarmes crítiques, generades tant per avaria hardware, per pèrdua d'alimentació elèctrica i per superació de límits de tràfic suportat o rendiment d'equip o ocupació de memòria (thresholds o llindars d'alarma).

El proveïdor, d'acord amb el CMPSB, determinarà quines són aquestes alarmes durant la fase de migració. Com a mínim s'hauran de contemplar les següents:

- Alertes sobre la pèrdua d'alimentació.
- Alertes sobre caigudes del sistema de ventilació en equips d'agregació, core i tallafocs.
- Avaria en elements clau, processadors, memòria, etc. dels equips d'agregació, core i tallafocs i commutadors de quiròfans i unitats de vigilància o cures intensives.
- Caiguda d'enllaços de xarxa WAN.
- Thresholds, alarmes per superació de nivells de tràfic en determinats enllaços i/o per tipus de protocol.
- Thresholds, alarmes per superació de nivells de rendiment o ocupació d'elements crítics com processadors i memòries.
- Detecció d'intrusions i atacs.
- Alertes relacionades amb els firewalls de CPD

Les alarmes molt crítiques es remetran als responsables del CMPSB per correu electrònic i/o a una app del smartphone.

Es calcula que hi haurà al voltant de 50 alarmes que s'han de tractar com a molt crítiques. En qualsevol cas, el proveïdor proposarà una llista d'alarmes crítiques.

Es desitja que el proveïdor actuï de manera proactiva detectant l'avaria o alerta abans que el CMPSB en almenys un 75% de les ocasions.

S'informa que actualment el CMPSB disposa i utilitza la versió gratuïta de la plataforma de gestió d'infraestructures tecnològiques Nagios i els seus tècnics estan formats i experimentats en l'ús d'aquesta plataforma. La plataforma proposada pel proveïdor ha d'integrar-se i sincronitzar-se amb la plataforma Nagios.

Malgrat el que s'ha indicat anteriorment, el CMPSB desitja disposar del màxim de prestacions i eines de gestió.

El proveïdor indicarà clarament quina plataforma utilitzarà i quines prestacions ofereix. Entre altres coses, es desitja que permeti com a mínim:

- Fer de manera automàtica el mapa topològic de la xarxa. Capacitat de "descobrir" la xarxa.

- Detectar la connexió de nous equips de xarxa.
- Actualització automàtica per a la correcció d'errors, actualitzacions de seguretat i noves característiques.
- Eines d'anàlisi de tràfic en temps real, com la captura de paquets i la prova de cables per aïllar i solucionar problemes de xarxa. Si és necessari el proveïdor instal·larà les sondes necessàries per comprovar possibles problemes de lentitud, STP i altres problemes de xarxa.
- Registre, logs, dels canvis de configuració dels equips.
- En els equips "zero touch provisioning", auto-desplegament, auto-configuració. En cas de substitució, es podrà configurar automàticament la recàrrega de la configuració sense intervenció de l'operador. Indicar quins equips instal·lats permeten aquesta prestació.
- Perfilatge de dispositius, és a dir, reconeixement del tipus de dispositiu i el seu sistema operatiu, i disposar de la possibilitat d'aplicar polítiques basades en dispositiu i/o sistema operatiu.

3.3. Manteniment preventiu.

Amb una periodicitat trimestral es durà a terme una visita a tots els racks i centres de dades del CMPSB que, com a mínim, contemplarà els següents aspectes:

- Procedir a netejar amb aire a pressió tots els ventiladors i sistemes de refrigeració dels equips.
- Comprovar la neteja dels nodes.
- Verificar que no s'han efectuat canvis físics ni hi ha hagut intents de manipulació dels equips.
- Comprovar que els cables de connexió, cables de connexió curts, etc., estan ben ordenats i identificats correctament.
- Comprovar que els protocols d'accés i seguretat físic s'apliquen correctament.
- Es fotografiaran tots els nodes i es remetran al CMPSB aquestes fotografies que també s'incorporaran als informes corresponents.

El proveïdor presentarà la seva pròpia proposta de tasques de manteniment preventiu que inclogui com a mínim els punts indicats anteriorment.

3.4. Manteniment correctiu

El servei de manteniment es durà a terme d'acord amb els següents paràmetres:

- Període de cobertura: segons l'horari de cada centre, indicat a l'Annex I d'aquest PPT.
- Electrònica d'accés: temps de reposició del servei de 4 hores dins del període de cobertura de cada centre.
- Xarxa Wi-Fi: temps de reposició del servei de 4 hores dins del període de cobertura de cada centre.

- Electrònica d'agregació: 24x7x4. Període de cobertura: tots els dies de l'any. Temps màxim de reposició del servei: 4 hores.
- Electrònica de DataCenter: 24x7x4. Període de cobertura: tots els dies de l'any. Temps màxim de reposició del servei: 4 hores.
- Tallafocs perimetrals i de CPD: 24x7x4. Període de cobertura: tots els dies de l'any. Temps màxim de reposició del servei: 4 hores.

El manteniment correctiu, a causa d'avaria hardware, inclou el reemplaçament d'equips, targetes o altres components avariats per elements iguals o compatibles de majors prestacions.

L'objectiu és que es reposi el servei amb les mateixes o superiors prestacions a les que es gaudia abans de la incidència o avaria, encara que no s'utilitzi un equip del mateix model, sempre del mateix fabricant.

4. Servei suport a l'administració

4.1. Help Desk

El proveïdor, com a part del servei que ha de prestar, posarà a disposició del CMPSB un servei de suport telefònic o Help Desk per a la resolució de dubtes o prestar suport als administradors de la xarxa. El servei es prestarà en català i/o castellà, els dies laborables de 8 a 17 h., com a mínim.

4.2. Suport a l'administració

El proveïdor, com a part del servei que ha de prestar, posarà a disposició del CMPSB un equip de tècnics qualificats per a suport en l'administració de la xarxa, altes, baixes, modificacions, etc., de forma remota o presencial. El servei es prestarà en català i/o castellà.

Les sol·licituds de suport que es puguin prestar remotament s'atendran en un màxim de 12 hores de dilluns a divendres de 8 a 21 hores.

Les actuacions que requereixin presència física als centres del CMPSB s'atendran en un màxim de dos dies laborables.

4.3. Còpies de seguretat

Dins del pla de migració es faran còpies de seguretat de la configuració de tots els equips de la xarxa. Les còpies es guardaran en dues ubicacions diferents: en el servidor del CMPSB assignat, ubicat al centre de dades principal, i en un servidor del proveïdor.

Es configuraran els equips de manera que automàticament, cada vegada que es faci una modificació, s'actualitzi la còpia de seguretat de l'equip a les dues ubicacions previstes.

Si no és possible la còpia 100% automàtica, s'establirà un procediment d'actuació per actualitzar totes les còpies de forma regular. La periodicitat amb què es faran les còpies dependrà de la periodicitat amb què es fan els canvis.

També es farà regularment una còpia de seguretat de la configuració de la plataforma de monitorització, dels nivells d'alarma establerts, del tipus d'informes que s'emeten, etc. Aquesta còpia també es farà en un servidor del CMPSB i un altre del proveïdor.

4.4. Gestió de versions

El proveïdor serà responsable de mantenir tots els equips actualitzats i de carregar totes les actualitzacions de programari, pegats, etc.

Pel que fa als tallafocs, també serà l'encarregat de mantenir tots els patrons i polítiques de seguretat actualitzades.

Totes aquestes actualitzacions es faran de forma programada i amb la prèvia autorització de l'administrador de la xarxa.

4.5. Suport enfront d'atacs externs i instruccions

Pel que fa a la ciberseguretat, el proveïdor haurà de responsabilitzar-se de detectar atacs i intents d'intrusió a la xarxa de qualsevol origen, entre altres:

- A través de la connexió a Internet.
- A través de connexions Wi-Fi del servei Hot-spot públic o intents de connexió de dispositius no autoritzats al Wi-Fi corporatiu.
- Per connexió d'algun dispositiu no autoritzat a alguna presa del sistema de cablejat.

El proveïdor ha de justificar que disposa de recursos adequats per fer front a aquestes incidències.

4.6. Informe de gestió i estadístiques d'ús

L'empresa gestora elaborarà mensualment un informe de gestió que ha d'incloure com a mínim la següent informació:

- Nombre d'actuacions de manteniment realitzades classificades per tipus.
- Informe de resolució de les incidències molt greus, causes i actuacions fetes i recomanacions perquè no es reprodueixi la incidència.
- Nombre d'actuacions d'administració realitzades: Altes, Baixes, Modificacions, etc., i el temps dedicat a les mateixes.
- Estadístiques de tràfic dels segments Ethernet o enllaços crítics.
- Estadístiques de tràfic dels enllaços crítics de la WAN: ocupació màxima, mínima i mitjana de cada segment mesurats en períodes de 5 minuts.
- Estadístiques de tràfic de la connexió a Internet: ocupació màxima, mínima i mitjana de cada segment mesurats en períodes de 5 minuts.
- Rendiment dels principals equips: commutadors core, commutadors de data center, tallafocs i commutadors d'accés molt crítics, com quiròfans i UVI. (Ex. Switch)

L'informe serà emès de forma electrònica, en PDF o Microsoft Office.

El proveïdor indicarà en la seva oferta l'índex d'aquest document que emetrà mensualment i que haurà d'incloure almenys els aproximadament 50 paràmetres o alarmes crítiques estimades.

Aquest informe s'emetrà dins dels 10 primers dies del mes següent.

4.7. Informe d'explotació

Anualment, s'emetrà un informe d'explotació amb almenys el següent contingut:

- Resum de les actuacions efectuades tant de manteniment com de suport a l'administració.
- Resum de les estadístiques d'ús emeses. Gràfiques d'evolució dels elements o paràmetres crítics.
- Proposta de millora i recomanacions d'inversió convenientment justificades.
- Avisos relatius a la vida dels equips i el suport que ofereix el fabricant i el que ofereix el proveïdor.
- Nivell de compliment SLA.

Aquest informe s'emetrà abans de 30 dies, finalitzats els períodes anuals, que no tenen per què coincidir amb l'any natural.

4.8. SOC Serveis Gestionats de Seguretat

Tots aquests serveis s'hauran de coordinar i conciliar amb el servei de Sistemes del CMPSB, assegurant una integració eficient i fluida en els processos existents. Aquesta col·laboració garantirà que qualsevol intervenció, actualització o resolució d'incidents es realitzi seguint els procediments establerts pel servei de Sistemes, mantenint la coherència amb les polítiques de seguretat, les infraestructures tecnològiques i les operacions diàries del CMPSB. A més, serà essencial establir una comunicació constant per assegurar que les actuacions dels diferents equips no interfereixin amb les tasques crítiques o comprometin la disponibilitat dels sistemes.

Serveis 24hX7d

- Vigilància d'infraestructures
    - Supervisió permanent dels paràmetres associats a l'estat i la disponibilitat de les infraestructures de seguretat.
    - Desencadenament d'alertes davant situacions anòmales o desviacions respecte als valors de referència definits, per a la detecció preventiva de sobrecàrregues i d'elements infrautilitzats.
- Gestió d'Alertes (SIEM)
    - Recollida i emmagatzematge de l'històric de registres generats pels equips de seguretat per a la seva anàlisi posterior.
    - Correlació avançada d'esdeveniments: Detecció d'atacs, vulnerabilitats, virus, accessos no autoritzats, atacants, equips atacats, patrons de comportament… i les hores en què es produeixen, determinant la criticitat, rellevància i falsos positius.

- Anàlisi, filtratge i qualificació de les alertes de seguretat detectades en base a una escala de risc.

- Resposta davant incidents
  - Execució de procediments de comunicació, actuació i escalat.
  - Primer nivell de diagnòstic, mitigació i escalat per part de l'Equip de Resposta davant Incidents.
  - Mitigació experta o de segon nivell davant incidents de major complexitat (diagnòstic profund i involucració de tot el personal de suport expert per a la neutralització i recuperació total dels sistemes afectats).
  - Sistema d'automatització de contramesures per a la contenció i mitigació de l'impacte davant amenaces habituals o conegudes.
  - Registre de documentació i emmagatzematge en BBDD d'incidents coneguts (amenaces, evidències, procediments, mesures correctives aplicades per a la resolució dels incidents detectats, …).

Mensual

- Gestió d'informes
  - Informe d'incidències (desglossament per classificació, prioritat i tecnologia), acumulat estadístic històric i tendències.
  - Inventari monitoritzat (Nom, model, IP, Número de sèrie, Versió de firmware, localització de xassís i targetes, altes i baixes).
  - Informe d'incidents i esdeveniments de seguretat significatius (procedència, criticitat, topologia, atacs i falsos positius/negatius).
  - Resta de capítols dedicats a cadascun dels serveis inclosos.
  - Butlletins de seguretat: Tendències del mercat, nous atacs, possibles noves vulnerabilitats, etc.
  - Quadres de comandament: Accés remot i segur a un portal únic i personalitzat amb la representació gràfica i lògica en temps real de paràmetres crítics del servei.

Serveis semestrals

- Gestió de Vulnerabilitats
  - Escaneig automàtic d'equips:
    - Anàlisi periòdic de vulnerabilitats sobre equips per detectar ports oberts i vulnerabilitats reportades. Escaneig i anàlisi des de dins i fora de la subxarxa en estudi (intranet / extranet). Informe automàtic de recomanacions tècniques i operatives per a la resolució de les vulnerabilitats identificades.
  - Servei d'alerta:

- Recopilació, anàlisi i emmagatzematge d'informes de vulnerabilitats emesos pels fabricants. Explotació de sistemes d'informació compartida per a la recollida de feeds relatius a malware, fonts de reputació i incidents de seguretat. Retroalimentació de BBDD d'intel·ligència contra amenaces de la plataforma SIEM per a una major efectivitat en la detecció d'amenaces.

4.9. Suport gestió xarxes WiFi

El proveïdor tindrà capacitat de prestar suport en l'administració de la xarxa Wi-Fi tant:

- Accés inalàmbric a la LAN interna de l'hospital per al personal sanitari.
- Accés públic a Internet per a pacients i visites (servei Hot-spot), que està actualment gestionat des de la plataforma de meraki.

Pel que fa al servei Hot-spot, s'haurà de tenir capacitat per donar suport en relació, entre altres, als següents aspectes, tant en la infraestructura Meraki com en l'antiga:

- Garantir que ambdós serveis, públic i corporatiu, tot i que comparteixen els mateixos equips, estan completament aïllats a nivell lògic i el tràfic prioritzat adequadament, sempre en detriment del tràfic de hot-spot.
- Control d'accés de visitants i pacients mitjançant codis d'autorització temporal.
- Control de navegació, bloqueig de webs, etc. Filtrat d'accés a continguts il·legals i altres que es determinin.
- Registre de navegació segons la legislació vigent.
- Bloqueig/autorització de serveis, per exemple, streaming de vídeo, descàrregues de fitxers de grans dimensions, etc.
- Protecció entre usuaris.
- Capacitat d'assignar un cabal màxim total del servei.
- Capacitat d'assignar un cabal màxim per usuari.
- Pantalla de benvinguda al servei i d'acceptació de condicions.
- Protecció enfront d'intrusions. Tenir en compte que l'Hospital del Mar es troba davant la platja, en una zona amb gran afluència de públic.
- Ajust, preferentment de forma automàtica, de tots els Access Points que componen la xarxa, especialment en els aspectes relatius a la ràdio, freqüència, canals, etc. Establir, de forma automàtica, la potència de transmissió i el canal de cada Access Point.
- Detecció automàtica de connexions d'antenes no autoritzades.
- Detecció d'interferències amb altres xarxes.
- Capacitat de crear mapes de cobertura.

- Monitorització del rendiment del sistema, etc.
- Detecció d'intents d'intrusió.
- Autenticació mitjançant usuari i contrasenya integrat amb Active Directory.

Com a part de l'estudi de situació, s'haurà de comprovar l'estat de tots els aspectes relacionats a continuació i solucionar les deficiències detectades i efectuar les recomanacions de millora oportunes.

L'estudi de situació també contemplarà la possible integració a efectes de gestió de les dues xarxes Wi-Fi.

Addicionalment, el proveïdor tindrà capacitat per donar suport en el desplegament i administració sobre la xarxa Wi-Fi dels següents serveis:

- Serveis d'analítica de localització sense necessitat de llicències addicionals ni maquinari addicional.
- Serveis d'analítica de presència d'usuaris, que permeti controlar els fluxos de persones i l'afluència de públic a les instal·lacions i les seves diferents àrees.

5. Governance

El CMPSB desitja establir un entorn de col·laboració eficaç amb el proveïdor que garanteixi un alt nivell de disponibilitat de la xarxa, minimitzant els riscos d'incidències i avançant-se als riscos d'obsolescència i/o falta de capacitat.

Per a això, és imprescindible establir una comunicació fluida i uns procediments de coordinació simples, clars, concrets i eficaços. Per tant, l'ofertant presentarà, acompanyant la seva oferta, una proposta completa de governança del servei. Aquesta proposta inclourà una relació de procediments de coordinació i el seu desenvolupament. Entre altres, es desenvoluparan els següents procediments:

- Gestió d'incidències:
  - A la xarxa WAN.
  - LAN.
  - Per sobrepassar llindars de tràfic o rendiment dels equips.
- Còpies de seguretat.
- Actualitzacions de versions de programari.
- Obertura d'incidències de forma manual.
- Suport d'administració.
- Accés a Help Desk.
- Accés a les instal·lacions del CMPSB.

6. Contractes, garanties, i acords de nivell de servei

L'objectiu dels serveis contractats a través d'aquest plec és que el CMPSB assoleixi un alt grau de disponibilitat de la xarxa. Es desitja assolir una disponibilitat global mínima del 99,5%, és a

dir, que la xarxa estigui completament operativa durant tot l'any, 24 hores al dia, el 99,5% del temps.

Per tant, el requeriment de nivell de serveis SLA (de l'anglès Service Level Agreement) tindrà un horari de cobertura de 24x7 amb un temps màxim de resposta de 4 hores. Aquest acord contemplarà nivells de servei global i per cada un dels components del servei:

Manteniment preventiu i correctiu:

- Capa d'accés
- Wifi corporativa
- Wifi pública
- Capa d'agregació
- Capa Data Center
- Tallafocs
- Monitorització remota
- Help Desk
- Suport a l'administració
- Còpies de seguretat
- Emissió d'informes:
- Estadístiques mensuals d'ús
- Informe anual

El contracte proposat contemplarà penalitzacions per incompliment dels nivells de SLA i especificarà els instruments de control dels mateixos i totes les fórmules de càlcul.

L'incompliment reiterat de les SLA global o de dos corresponents a altres components del servei durant tres mesos consecutius o 6 alterns durant un any, habilitarà el CMPSB a rescindir unilateralment el servei sense compensar el proveïdor de cap manera.

El CMPSB valora els compromisos que s'adquireixen en aquest punt i les penalitzacions proposades. (Punt 14.2.4 del PCA)

7. Pla de migració i activació del servei

7.1. Direcció

El present projecte és responsabilitat de la Direcció de Sistemes d'Informació i comunicacions del CMPSB, que nomenarà un administrador de la xarxa com a interlocutor principal amb el proveïdor.

7.2. Responsable del servei

L'adjudicatari nomenarà un responsable del servei, que serà l'interlocutor principal amb l'administrador de la xarxa.

El responsable del servei assistirà a les reunions de seguiment a què el convoqui el CMPSB, aproximadament una per trimestre. Durant el primer semestre d'operació del servei, les reunions tindran una freqüència superior, amb un màxim d'una al mes.

Assistirà a les reunions de coordinació amb altres possibles proveïdors del departament de sistemes a què se'l convoqui, especialment amb el proveïdor de la WAN.

7.3. Equip de treball

S'indicarà la composició del grup de treball, la seva experiència, l'organigrama, el perfil dels treballadors que destinaran al servei objecte del contracte i on es demostri que compleixen amb els requisits mínims sol·licitats al PPT.

L'equip disposarà d'un mínim de 8 tècnics amb base a l'àrea metropolitana de Barcelona. Es demana que la licitadora disposi d'una base (oficina o taller) a l'àrea metropolitana de Barcelona, encara que la seva central pugui estar ubicada en qualsevol altra població. Aquesta sol·licitud es fonamenta en la necessitat de complir amb l'SLA establert, que exigeix un temps màxim de resolució de 4 hores, donada la naturalesa crítica del servei.

Es facilitarà l'historial professional de tot el personal pertanyent a l'equip de treball on s'indicarà quins certificats dels fabricants disposen i la seva data d'obtenció i caducitat.

El grup de treball estarà subjecte a la prèvia conformitat del CMPSB.

Els tècnics assignats al grup de treball hauran de comptar amb una experiència acreditada mínima de dos anys en l'àmbit objecte d'aquesta licitació. Aquesta experiència es justificarà mitjançant la presentació del Currículum Vitae corresponent.

El grup de treball haurà de comptar, en conjunt, amb la formació certificada corresponent, acreditada mitjançant les certificacions oficials de Cisco, Fortinet i Palo Alto.

Els certificats mínims sol·licitats son els següents :

Cisco :

- CCNA.
- CCNP Enterprise.
- CCNP Service Provider.
- Cisco Certified Specialist – Enterprise Advanced Infraestructure Implementation.
- Cisco Certified Specialist – Enterprise Core.
- Cisco Certified Specialist – Enterprise Desing.
- Cisco Certified Specialist – Service Provider Advanced Routing Implementation.
- Cisco Certified Specialist – Service Provider Core.
- Cisco Certified Specialist – Service Provider VPN Services Implementation.
- Cisco Customer Success Manager.

Fortinet:

- Fortinet Certified Fundamentals in Cybersegurity.
- Fortinet Certified Professional Network Security.
- Fortinet Certified Solution Specialist Network Security.

Palo Alto:

- Palo Alto Networks Certified Network Security Engineer PCNSE
- Palo Alto Networks Certified Software Firewall Engineer PCSFE
- Palo Alto Networks Accredited Systems Engineer - Software Firewall Professional
- Palo Alto Networks Systems Engineer Professional Strata
- Palo Alto Networks PSE: SASE Professional

7.4. Activació del servei

L'adjudicatari assumirà el servei de manteniment correctiu de la xarxa abans de 15 dies naturals a partir de la formalització del contracte. Disposarà d'un termini de 3 mesos a partir de la formalització del contracte per activar la totalitat dels serveis previstos.

7.5. Pla de migració

El licitador haurà de presentar una proposta de pla de migració o llançament del servei, que descrigui el programa detallat de treball que estimi més oportú i que garanteixi que està preparat per assumir el manteniment i les tasques de suport a l'administració d'acord amb el que es preveu en aquest plec.

El procés de migració ha de contemplar obligatòriament les següents tasques:

- Estudi de situació amb el següent contingut mínim:
    - Documentació AS-Built de la xarxa.
    - La configuració de tots els equips.
    - Diagrames de blocs.
    - Comprovació i documentació de l'alimentació elèctrica de tots els equips, incloent-hi el tipus de proteccions elèctriques, magnetotèrmics i diferencials.
    - Esquemes de connexió.
    - Funcionament dels hot-spots wifi.
    - Relació de recomanacions de millora per augmentar el rendiment, la fiabilitat i la disponibilitat de la xarxa.

- Activació del sistema de monitorització.
- Instal·lació de la consola del sistema de monitorització a les instal·lacions del CMPSB i integració i sincronització amb la plataforma Nagios.
- Instal·lació de l'app als telèfons intel·ligents del departament de sistemes.
- Incorporació, a nivell de lectura, dels equips de xarxa WAN de l'operadora de telefonia contractada pel CMPSB o qui pugui substituir-la en el futur.
- Actualització de les versions de programari dels equips.
- Còpies de seguretat de la configuració de tots els equips.
- Formació del personal de sistemes del CMPSB.
- Pla de migració per al traspàs del servei a un nou proveïdor una vegada finalitzat el període contractat.

La durada màxima del pla de migració s'ha establert en 10 setmanes; tot el procés des de la formalització del contracte ha d'estar finalitzat abans de 3 mesos.

El pla indicarà:

- Una relació detallada de les etapes i activitats a realitzar amb el resultat a obtenir en cadascuna d'elles, els recursos assignats i la documentació a emetre. El pla no ha de

provocar indisponibilitat de la xarxa actual, ja que aquesta és crítica per a l'operativa de l'Hospital.

- Calendari detallat del projecte.
- Proves d'acceptació i procediments de control de qualitat.
- Pla de seguretat i salut en el treball adaptat als serveis que es prestaran, d'acord amb els requisits establerts per la legislació vigent.

7.6. Col·laboració lleial

El present servei és una part crítica de l'operativa del CMPSB, en la qual col·laboren diferents empreses. El licitador ha de comprometre's a col·laborar lleialment amb aquestes empreses, encara que es tracti d'un competidor directe. Haurà de col·laborar especialment amb l'operador de telefonia actual com a proveïdor de la xarxa WAN o amb l'operador que el pugui substituir en el futur.

El proveïdor col·laborarà lleialment amb l'empresa que el substitueixi una vegada finalitzat el contracte, en cas de no resultar adjudicatari de la següent licitació.

7.7. Proves d'acceptació

El CMPSB podrà realitzar per si mateixa o amb suport extern les auditories i inspeccions que consideri oportunes abans d'acceptar l'inici del servei i durant la seva durada.

L'ofertant presentarà un pla detallat de Proves d'acceptació que garanteixin que presta el servei conforme al previst en les presents especificacions.

El proveïdor, en presència del CMPSB i eventualment dels assessors que aquesta consideri oportuns, demostrarà el perfecte funcionament de la plataforma de monitorització. El proveïdor aportarà, si és necessari, la instrumentació que es requereixi per a aquest fi, com ara elements de generació de tràfic, etc.

Les proves d'acceptació no hauran d'afectar al normal funcionament de la xarxa.

A continuació, es relacionen els aspectes que obligatòriament ha d'incorporar el pla d'acceptació:

- Detecció de la caiguda d'un enllaç.
- Detecció d'un intent d'intrusió per l'enllaç d'Internet.
- Detecció d'un atac de DOS sobre els servidors públics del CMPSB.
- Correcta configuració dels Sistemes de Gestió.
- Protecció contra intrusió de la xarxa Wi-Fi:
    - Entre usuaris del hot-spot o xarxa pública.
    - De la xarxa pública a la xarxa interna de l'hospital.
- Comportament dels equips davant la caiguda d'un enllaç.
- Canvi de ventiladors i fonts d'alimentació en calent.
- Comportament en cas de tall d'alimentació elèctrica.
- Simulació d'alts nivells de tràfic superiors als límits establerts.
- Control d'amplada de banda de la WAN i de l'enllaç a Internet.

- Identificació d'usuaris de hot-spot públic.

Es signaran les corresponents actes d'acceptació.

7.8. Documentació

El proveïdor haurà de lliurar, un cop finalitzat l'estudi de situació i abans de l'inici efectiu del servei, la següent documentació:

- Estudi de situació.
- Manuals d'ús de la plataforma de monitorització.
- Configuració de la plataforma de monitorització amb els nivells d'alarma determinats.
- Claus d'usuari per accedir a la plataforma de manuals i documentació dels fabricants.
- Documentació visual de la xarxa dels diferents centres i actualitzada com a mínim quatrimestralment.

Es recorda que al llarg del servei emetrà:

- Mensualment l'informe de gestió i estadístiques d'ús.
- Anualment l'informe d'explotació.

També es tramitarà i facilitarà l'accés a les plataformes de suport dels fabricants, que inclouen:

- Resolució de casos.
- Manuals actualitzats.
- Anuncis de noves versions, etc.

8. Formació

El CMPSB desitja que el seu departament de sistemes, actualment format per 4 persones, rebi formació continuada en tecnologies i gestió de xarxa. Per això, dins del servei sol·licitat s'inclourà:

1) Curs de formació inicial amb l'objectiu de:
    a) Capacitar-los en la utilització de la plataforma de monitorització remota i del seu potencial. Incloent aspectes com:
        i) Detecció i atenció immediata de les avaries, aprenent a discriminar l'element avariat o fora de servei i avaluar la importància de la mateixa.
        ii) Utilització de la plataforma perquè puguin programar i reconfigurar els equips, extreure informes d'utilització o tràfic, fer seguiment de les alarmes, realitzar la reposició del sistema, executar els programes de manteniment, etc.
        iii) Obtenir estadístiques de tràfic, tant puntuals, com regulars: disponibilitat, tràfic cursat i rebut pels diferents enllaços, etc.
    b) Comprensió dels procediments de coordinació amb el proveïdor.

2) Curs anual de formació contínua amb l'objectiu de:
   a) Conèixer els últims desenvolupaments i millores en tecnologies de networking IP i ciberseguretat.
   b) Conèixer les prestacions de les noves versions de programari dels equips.

Es facilitarà en l'oferta una proposta de contingut del curs de formació i dels certificats que es lliuraran als assistents.

Cal tenir en compte que els tècnics del departament de sistemes d'informació del CMPSB disposen d'amplis coneixements i una dilatada experiència en gestió de xarxes Ethernet. Per això, els cursos sol·licitats han de ser de nivell avançat. En cap cas es desitja assistir a cursos bàsics.

9. Ampliacions puntuals

El CMPSB, amb l'objectiu de solucionar ràpidament problemes relacionats amb el bon funcionament de la xarxa, pot precisar que l'empresa que presta el servei de manteniment i suport a l'administració tingui capacitat de subministrar i instal·lar equips nous de la capa d'accés i antenes per ampliar la xarxa sense fil WIFI.

El proveïdor proposarà els següents equips del mateix fabricant i compatibles amb els actuals:

- Commutador de 24 ports.
- Commutador de 48 ports.
- Antena punt d'accés.
- Ampliació d'equips CPD.

El model i preu de l'equip instal·lat s'actualitzarà anualment en funció de la paritat €/$.

Aquests equips s'incorporaran al servei de manteniment i suport a l'administració.

10. Presentació d'ofertes

10.1. Sobre número 2

El proveïdor haurà d'oferir un servei que compleixi fidelment les condicions i requeriments citats en aquestes especificacions.

Haurà de facilitar tota la informació necessària per garantir que està qualificat per prestar el servei sol·licitat.

Es presentarà l'oferta en suport informàtic estàndard, Microsoft Office i AUTOCAD, o PDF, amb l'estructura que es descriu en els següents apartats.

El contingut del sobre tècnic serà:

- Certificats del grup de treball, detallats al punt 7.3 d'aquest document.

- Compromís que es compleixen les especificacions i s'assumeixen els compromisos sol·licitats.

El sobre número 2 no incorporarà cap dada econòmica ni informació sobre els certificats dels fabricants.

Tota l'oferta haurà de ser clara, concreta i concisa, responent a tots els punts contemplats i en l'ordre exposat anteriorment. Es valoraran amb “0” zero punts aquelles ofertes que no compleixin estrictament aquests requisits.

10.2. Sobre número 3

S’haurà d’incloure l’oferta econòmica, de conformitat amb el model de l’Annex 2 del PCAP, i els certificats dels fabricants valorables d’acord amb el punt 14.1.2 dels Criteris avaluables de forma automàtica inclosos a l’Annex 4 del PCAP.

Barcelona, a la data de signatura electrònica

Pablo Andolz Cardó
Cap de Sistemes del CMPSB