Parc Taulí
Consorci Corporació Sanitària

PLEC DE CONDICIONS TÈCNIQUES PER A LA CONTRACTACIÓ DE L'EINA DE GESTIÓ UNIFICADA DEL LLOC DE TREBALL

EXPEDIENT: 24SER0881

ÍNDEX

1 Introducció

El Consorci Corporació Sanitària Parc Taulí de Sabadell és un consorci públic de la Generalitat de Catalunya, el màxim òrgan de govern del qual és el Consell de Govern, i que gestiona els següents centres: Hospital de Sabadell, UDIAT Centre Diagnòstic, Albada Centre Sociosanitari, Salut Mental Parc Taulí, Atenció Primària Parc Taulí, Atenció a la Dependència Parc Taulí, i també els serveis de Sabadell Gent Gran Centre de Serveis, a través d'una societat anònima. El Consorci és el soci únic d'aquesta darrera entitat i nomena a tots els membres del seu consell d'administració. A més a més, és Unitat Docent de la Facultat de Medicina de la Universitat Autònoma de Barcelona (UAB) i té la consideració d'Hospital Universitari.

El Consorci Corporació Sanitària Parc Taulí es troba vinculat a la Fundació Institut Investigació i Innovació Parc Taulí, el patronat de la qual nomena a la majoria de membres. Les institucions del Consorci reben el suport de la Fundació Parc Taulí en aspectes de recerca, innovació i docència, en la formació científica i mèdica dels professionals i, en general, en el desenvolupament dels coneixements que sustenten el model assistencial.

En aquest document ens referirem al Consorci Corporació Sanitària Parc Taulí com a **CCSPT**.

La missió del CCSPT és donar assistència resolutiva, integral, personalitzada i de qualitat als ciutadans de la seva àrea de referència tot fomentant l'equitat, la continuïtat assistencial, la satisfacció, l'eficiència i la sostenibilitat.

Actualment el CCSPT atén una població de referència de 407.864 habitants, disposant d'una infraestructura de 670 llits d'aguts i 196 llits sociosanitaris. Una mostra de la seva activitat assistencial serien les més de 400 urgències diàries de mitjana, més de 250 intervencions quirúrgiques diàries de mitjana o més de 2.700 consultes externes diàries, també de mitjana. Gestiona diverses empreses amb Convenis Col·lectius diferents (SISCAT, Oficines i Despatxos, Sociosanitari i Dependència) amb una plantilla mensual contractada d'aproximadament uns 4.300 professionals, que també inclou Sabadell Gent Gran (SGG) i la Fundació Institut d'Investigació i Innovació Parc Taulí (FI3PT).

2 Objecte del contracte

Contractació del servei d'implantació de l'eina de gestió unificada del lloc de treball (Unified Endpoint Manager - UEM)

3 Vigència del contracte

La vigència del contracte del servei serà aproximadament de 30 mesos, prorrogable anualment fins a un màxim de 2 anys més, a partir de la data de signatura del contracte.

La data d'inici de l'execució de contracte serà el dia següent al de la seva formalització

4 Abast del contracte

L'abast del subministrament és el següent:

PBL	Entitat	Exercici	Import net	% IVA	Import IVA	Import IVA inclòs
LOT – 1	CCSPT	2024	37.150,22 €	21%	7.801,55 €	44.51,77 €
		2025	74.300,43 €	21%	15.603,09 €	89.903,52 €
		2026	74.300,43 €	21%	15.603,09 €	89.903,52 €
	SGG	2024	1.043,41 €	21%	219,12 €	1.262,53 €
		2025	2.086,82 €	21%	438,23 €	2.525,06 €
		2026	2.086,82 €	21%	438,23 €	2.525,06 €
	I3PT	2024	1.479,82 €	21%	310,76 €	1.790,58 €
		2025	2.959,64 €	21%	621,52 €	3.581,16 €
		2026	2.959,64 €	21%	621,52 €	3.581,16 €
TOTAL LOT-1			198.367,23 €		41.657,12 €	240.024,35 €

5 Condicions específiques del contracte

L'oferta es farà per la totalitat dels elements que componen el LOT. No s'acceptaran en cap cas ofertes parcials que no comprenguin tots els elements del LOT. L'oferta presentada no podrà ser superior a l'import total de la licitació del LOT.

A tots els efectes, s'entendrà que en l'oferta i en els preus proposats per l'adjudicatari s'inclouen totes les despeses que hagi de realitzar per al compliment del contracte (transport, taxes, treballs, garanties, accessoris i mà d'obra).

Els licitadors hauran d'aportar, dins del sobre digital, tant les fitxes tècniques del fabricant, com qualsevol altre documentació tècnica necessària que permeti validar els requeriments que el CCSPT detalla en aquest plec, així com la seva ubicació dins de la documentació aportada. En cas que falti aquesta informació o no es compleixi algun requeriment, el licitador quedarà exclòs.

Les comandes seran enviades per el CCSPT via email, en format PDF, a la direcció de correu electrònic que així indiqui l'adjudicatari.

6 Característiques Tècniques

6.1 Introducció.

Què és UEM?

UEM (de l'anglès Unified Endpoint Management), o gestió unificada de punts finals , és un programari per supervisar, gestionar i protegir tots els dispositius d'usuari final d'una organització (ordinadors d' escriptori i

portàtils, telèfons intel·ligents, tablets, dispositius portàtils i més) des d'una única consola, independentment del sistema operatiu o la ubicació . UEM reforça la seguretat dels punts finals simplificant-la , el que permet als equips de seguretat i TI protegir tots els dispositius de punt final utilitzant una sola eina de manera coherent .

Amb una tecnologia relativament nova , UEM combina les prestacions de les solucions de gestió mòbil existent, incloent MDM (Mobile Device Management: gestió de dispositius mòbils) i MAM (Mobile Application Management: gestió d' aplicacions mòbils), amb les de les eines utilitzades per gestionar PC en local i en remot . També per gestionar programes BYOD (Bring Your Own Device: porti el seu propi dispositiu) i plantilles híbrides (combinació de llocs de treballa en local i en remot), l'ús d'UEM s'ha disparat a mesura que els departaments de seguretat i TI s'estan adaptant per ampliar el suport al treball remot (des de casa) després de la pandèmia de COVID-19. Aquesta tendència sembla que es mantindrà en el futur proper.

L' evolució del UEM.

UEM és la més recent d'una sèrie d' eines de gestió de seguretat mòbil , que van sorgir i evolucionar en resposta als canvis en la relació entre organitzacions, empleats , dispositius mòbils i estils de treball en les darreres dues dècades.

Com UEM millora la seguretat dels punts finals.

L'ús de diverses eines de gestió de punts finals per gestionar i protegir diferents dispositius en diferents ubicacions genera una gran quantitat de treball manual i repetitiu per als equips de seguretat i de IT, a més d' augmentar la probabilitat d' inconsistències , errors de configuració i una altra classe d' errors que poden deixar exposats als punts finals i la xarxa a possibles atacs. UEM redueix en gran mesura el treball i el risc mitjançant la creació d'un únic panell de control central on els administradors de TI i els equips de seguretat poden veure, gestionar i protegir *tots* els dispositius connectats a la xarxa empresarial.

Les eines de UEM funcionen en tots els sistemes operatius de PC i mòbils , inclosos Apple iOS i MacOS , Google ChromeOS i Android , Linux i Microsoft Windows (algunes solucions també són compatibles amb els sistemes operatius mòbils Blackberry US i Windows Phone). Moltes solucions de UEM també admeten impressores i altres dispositius de IoT d'usuari final, rellotges intel·ligents i altres dispositius wearables , cascos de realitat virtual, assistents virtuals, en definitiva qualsevol cosa que un empleat o business partner pugui utilitzar per connectar-se a la xarxa i fer la seva tasca.

UEM controla tots els dispositius a la xarxa, independentment del tipus de connexió, la freqüència amb què es connecten i des d'on es connecten. Fins i tot pot detectar dispositius connectats que els administradors o equips de seguretat no coneixen, en temps real.

6.2 Requeriments

El CCSPT pretén acomplir els següents requisits, amb la incorporació d'una eina de gestió del lloc de treball.

Des d' aquest tauler de control central, els administradors poden realitzar o automatitzar tasques de gestió i seguretat crítiques per a qualsevol dispositiu, o per a tots ells, incloent :

- **Inscripció i subministrament de dispositius:** per reduir la càrrega administrativa de BYOD, les solucions de UEM proporcionen un portal on els usuaris poden autoinscriure's i subministrar els seus

dispositius automàticament . UEM també imposa automàticament la inscripció i el subministrament per a qualsevol dispositiu nou o desconegut que intenti connectar-se a la xarxa.

- **Aplicació i compliment de les polítiques de seguretat :** els administradors poden especificar autenticació de multifactors, la longitud i la complexitat de les contrasenyes , renovacions de contrasenya , mètodes de xifratge de dades i molt més . En permetre que els administradors distribueixin polítiques coherents en tots els dispositius amb una sola eina , UEM redueix en gran mesura el treball manual per als departaments de IT i el personal de seguretat.

- **Aplicació de pegats i actualitzacions :** UEM pot analitzar els punts finals per detectar vulnerabilitats de programari, firmware o sistema operatiu i aplicar automàticament pegats on sigui necessari.

- **Control d' aplicacions :** els administradors poden aprovar o prohibir l'ús d'aplicacions específiques , i impedir que les que no estiguin autoritzades accedeixin a les dades empresarials . Moltes eines de UEM permeten crear una botiga d' aplicacions, on els usuaris poden descarregar, instal·lar i actualitzar periòdicament aplicacions d' escriptori i mòbils aprovades per l'empresa.

- **Aïllament de dades corporatius i dades personals :** amb això es protegeixen les dades corporatives i dades personals i es proporciona l' experiència de l' usuari òptima per a BYOD.

- **Mantenir actualitzades les solucions de seguretat de punts finals :** els administradors poden instal·lar les últimes definicions d'antivirus als dispositius, actualitzar els filtres web amb els darrer llocs web a la llista negra o la llista blanca i fins i tot ajustar els tallafocs per repel·lir les últimes amenaces. .

- **Protecció de connexions :** UEM permet als administradors especificar el tipus de connexió per exemple, wifi o VPN per dispositiu, per usuari o fins i tot per aplicació.

- **Identificació i correcció d' amenaces :** en integrar-se amb UEBA (User and Entity Behavior Analytics), detecció i resposta de punts finals (EDR) i altres tecnologies de seguretat, UEM pot ajudar a identificar comportaments anormals del dispositiu que indiquen amenaces en curs o potencials , i activar-ne d'altres eines de seguretat per prendre mesures contra elles.

- **Neteja i/o bloqueig de dispositius perduts , robats o al final del cicle de vida:** com a última línia de defensa, UEM permet als administradors o equips de seguretat, ubicar, netejar , bloquejar i restaurar dispositius perduts, robats o retirats, impedir l'accés no autoritzat a la xarxa i evitar que les dades sensibles del dispositiu caiguin a les mans equivocades. També pot restablir dispositius donats de baixa per a un ús personal posterior.

El principal avantatge és que per a aquestes i altres tasques, l'enfocament integral de UEM permet que els departaments de seguretat i IT ignorin les distincions entre dispositius dins i fora de la organització, dispositius d 'escriptori i mòbils, sistemes operatius Windows, Mac, Chrome o Linux, i simplement se centrin en la gestió de la seguretat i els dispositius.

Algunes capacitats comunes de UEM han d'incloure :

- Una interfície de panell únic per administrar dispositius d'escriptori, portàtils i mòbils.
- La interfície ha de ser en Castellà
- Possibilitat d'enviar actualitzacions de sistema operatiu als dispositius .
- Capacitat per aplicar polítiques de seguretat als dispositius administrats .

- Esborrat remot que pot suprimir totes les aplicacions i dades d'un dispositiu perdut o robat .
- Capacitats de gestió d'aplicacions. Enviar aplicacions empresarials a dispositius administrats o proporcionar als usuaris autoritzats accés a una botiga d'aplicacions empresarials on l'usuari pot descarregar aplicacions pel seu compte .
- Visibilitat sobre tota la xarxa de IT i informe als administradors sobre qualsevol possible problema en dispositius Windows, macOS i Linux, andorid, IOS.
- Implementació simplificada. Aprofitar les solucions dissenyades per al núvol per facilitar la instal·lació. Possibilitat d'accedir-hi mitjançant una interfície web. Als dispositius, es despleguen agents de supervisió per afegir-los al panell.
- Diversitat d'endpoints. Administrar dispositius de xarxa com impressores, routers, tallafocs i dispositius mòbils (portàtils, equips d' escriptori, telèfons, tauletes), i supervisar i administrar altres endpoints rellevants (dispositius IoT, electromedicina) a través de la xarxa SSH.
- Millorar l'experiència com a administrador de IT. Administrar mitjançant un panell únic: els agents comuniquen els estats dels dispositius al programari, que dur a terme comprovacions i tasques amb la freqüència desitjada .
- Aplicació de pegats. Aplicar pegats en qualsevol entorn de xarxa , de forma programada o sota demanda desplegant-los a les xarxes , dispositius o grups .
- Accés remot. Accedir a qualsevol dels seus endpoints per oferir assistència remota, de forma àgil, a través d'un únic panell de control centralitzat .
- Automatització. Accediu a centenars de scripts desenvolupats de manera interna o per altres clients que estan usant característiques d'automatització, per a la resolució de les incidències mes comunes.
- Administració de dispositius mòbils. Faciliteu la supervisió, manteniment i seguiment dels dispositius mòbils propietat tant dels empleats com de l'empresa.
- Elaboració d'informes. Genereu informes sòlids que facilitin la implementació de l'estratègia de IT i empresarial.
- Ajustament d'escala. Cal afegir tants endpoints com la corporació necessita a cada nivell .
- Un sistema amb diversos productes. Incloeu característiques essencials addicionals en un únic sistema: antivirus, dispositiu tallafocs, administració de contrasenyes, seguretat del correu electrònic i moltes més .
- Integracions. Integrar les solucions preferides d' administració de IT empresarials amb integracions llistes per utilitzar o mitjançant API. Integrar amb JIRA Services Desk.
- Formació. Formar als administradors IT de l'eina en l'administració i configuració de la mateixa i l'ús i gestió dels dispositius dels entorns de treball a través de l'eina.
- El CCSPT té en productiu el següent nombre de dispositius a gestionar:
    - 1053 impressores
    - 2652 ordinadors fixes
    - 703 portàtils
    - 71 tablets
    - 68 players (ordinadors de pantalles cues)
    - 11 dispensadors (ordinadors gestió cues)
    - 57 TV intel·ligents
    - 8 docsstations
    - 462 telèfons mòbils gestionables (10 apple, 452 android).
    - Properament s'incorporaran fins a 300 escriptoris "virtuals" facilitadors del teletreball que també s'hauria de gestionar a nivell d'incidència.
- Els Sistemes operatius mes estesos: Windows 10, IOS (darrera versió), android (varies versions). En menys proporció: Windows 11, Windows 7.
- Aquests dispositius es troben en diferents subxarxes i, n'hi ha que disposen de mobilitat i treballen en remot.

- Disposem d'un EDR (Trellix) instal·lat en tots els ordinadors, Que s'ha de distribuir a través de l'eina i facilitar l'accés al portal de gestió.
- Els usuaris es validen de forma inequívoca als ordinadors amb un usuari personal creat al AD.
- Es disposa d'una eina de distribució de paquets i configuracions (ZENWorks). Els paquets de distribució de software s'hauran de traslladar al nou entorn.
- S'apliquen polítiques de seguretat del AD.
- S'ha d'integrar amb les eines de gestió de suport: JIRA: portal d'incidències i CMDB de maquinari. Enllaçar dispositius i mantenir l'inventari actualitzat.

7 Garanties

- L'adjudicatari ha de disposar i proporcionar un servei d'atenció telefònica i una persona de contacte per tal de poder gestionar les incidències relacionades.

- Ha d'existir un suport d'evolutius i dubtes que acolli 100 hores tècniques des de la posada en producció de la plataforma. L'horari de resposta serà de 2 dies laborables, i el de resolució de la petició de 6 dies laborables.

	Terminis
Volum d'hores de Suport	100 hores tècniques
Temps de resposta	2 dies laborables
Temps de resolució	6 dies laborables

- En cas d'incidències , si no s'especifica un SLA més restrictiu, el temps de resposta, definit com el període màxim de temps entre la notificació de l'avaria i la resposta d'un tècnic especialitzat, serà de 8h laborables. El temps de resolució, definit com el període màxim de temps entre la notificació de la incidència, ja sigui per resolució de l'avaria o per substitució del material, no ha de ser superior a 48h laborables.

	Terminis
Temps de resposta	8h laborals
Temps de resolució crític	16h laborals (2 dies)
Temps de resolució	48h laborals (6 dies)

8 Documentació de lliurament

Amb l'entrega de l'entorn, caldrà proporcionar la documentació relacionada amb:

- La formació específica d'administració i gestió

- L'estat i configuració de l'entorn
- Procediments estandarditzats de primer nivell (alta, baixa, canvi, control remot, automatització de tasques, etc...)

9 Suport Configuració

Per tots els elements objecte d'aquest plec, és imprescindible i obligatori que el software associat, ofert pel licitador, sigui completament compatible amb totes les aplicacions i la infraestructura utilitzats en el CCSPT.

A més, l'adjudicatari haurà de donar suport en la configuració, segons requisits del CCSPT si és necessari, per tal de que el comportament dels dispositius s'ajusti a les aplicacions i la infraestructura en els que s'empraran els diferents aparells, si s'escau.

10 Qualitat i Mediambient

El material de la present licitació ha de ser conforme, en el moment del lliurament, amb la normativa vigent de la Unió Europea i de l'Estat pel que fa a aspectes de qualitat, ergonomia, medi ambient, estalvi energètic, compatibilitat electromagnètica, reducció de la petjada CO_2 emesa i seguretat, així com a normatives de disseny, fabricació, embalatge i etiquetatge.