PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGIRAN A LA CONTRACTACIÓ D'UN SERVEI GESTIONAT DE DETECCIÓ I RESPOSTA D'AMENACES AVANÇADES (MDR) AL CONSORCI SANITARI DEL MARESME

EXPEDIENT CSdM 19/25-I

IMP-SC-006

ÍNDEX

1 INFORMACIÓ GENERAL DEL CONSORCI SANITARI DEL MARESME

El Consorci Sanitari del Maresme, en endavant CSdM, és una entitat en la qual participen el Servei Català de la Salut, el Consell Comarcal del Maresme i l'Ajuntament de Mataró.

L'objectiu del Consorci és l'execució d'activitats hospitalàries, assistencials, preventives, rehabilitadores, docents i d'investigació al servei de la població resident en l'àmbit sanitari de la comarca del Maresme i la seva àrea sanitària d'influència.

Són finalitats específiques del Consorci, l'assistència hospitalària integrada, vinculada a la xarxa d'assistència primària i coordinada amb altres nivells sociosanitaris, la prestació de serveis d'atenció primària de salut, la prestació de serveis de salut mental i la prestació de serveis d'atenció sociosanitària i social, la participació en la promoció de campanyes o tasques de medicina preventiva, proporcionar serveis de rehabilitació, la docència relacionada amb la sanitat i, en general, en matèria de salut física i mental.

Es pot complementar la informació descrita en aquest plec des de la pàgina web del CSdM http://www.csdm.cat

2 OBJECTE DEL CONTRACTE

2.1 Objectiu i abast.

El present document, que formarà part del contracte, té la finalitat de descriure les tasques a desenvolupar per part de l'empresa adjudicatària per tal de que aquesta pugui presentar proposta tècnico-econòmica per la realització dels treballs encarregats.

L'objecte d'aquesta contractació és:

- Llicenciament d'ús d'una solució MDR en modalitat SaaS per la protecció contra amenaces avançades en **1.700 estacions de treball i 240 servidors** del CSdM, completament gestionats per l'adjudicatari.
- **Servei de SOC** per donar resposta al compliment dels requeriments d'aquest plec tècnic per la monitorització i resposta a alertes, gestió de la plataforma, actualitzacions, intel·ligència d'amenaces i funcionalitats avançades de detecció i resposta en modalitat 24x7x365.
- Manteniment i suport de la solució.
- **Subministrament, instal·lació, configuració i posada en marxa** d'una solució MDR per al CSdM**.**

Es definirà un **calendari de treball** amb el temps d'actuació, fites, aspectes tècnics i econòmics de tots els sistemes abans esmentats, serveis inclosos.

L'adjudicatari ha de fer una **proposta detallada dels serveis relatius a instal·lació, configuració i posada en marxa**, i com dur-los a terme, minimitzant l'afectació i el risc, sobretot en servidors, per l'assoliment dels requisits esmentats en aquest PPT i garantir l'èxit de l'encàrrec i la continuïtat del servei.

La proposta ha d'incloure tots els costos del projecte, en modalitat de pagament únic, amb **facturació trimestral**, i sense costos addicionals, i en funció del nombre d'estacions i servidors desplegats i en funcionament mensualment; essent un contracte amb preus unitaris, el Consorci no assumeix un compromís de contractar un nombre mínim d'unitats.

De manera complementària i subsidiària, i en tant no s'oposi al present plec, serà d'aplicació el contingut de l'oferta dels licitadors.

El no compliment dels requisits tècnics redactats en el present plec seran objecte d'exclusió de la present licitació.

2.2 Duració del contracte

La duració del contracte derivat d'aquesta licitació serà de **TRES (3) ANYS**, computat des de la data d'inici, una vegada rebuda la conformitat mitjançant la corresponent acta firmada per ambdues parts i **prorrogable anualment DOS (2) ANYS addicionals**.

2.3 Terminis d'execució

El termini màxim d'execució del projecte d'implementació serà de **TRES (3) MESOS**, computat des de la data d'inici, una vegada rebuda la conformitat mitjançant la corresponent acta firmada per ambdues parts, fins la data de finalització de la configuració de la consola i desplegament de la solució als equips del client.

La data d'inici del projecte s'haurà de definir, de mutu acord per ambdues parts i, en cap cas, haurà de ser posterior als **TRENTA (30) DIES NATURALS** des de la data de formalització del contracte.

3 ANTECEDENTS

Situació actual de la infraestructura del CSdM

Actualment, el CSdM disposa d'una infraestructura d'estacions de treball Windows i servidors Windows i Linux protegits amb una solució EPP tradicional del fabricant McAfee. Aquests estan gestionats i orquestrats de forma centralitzada en un servidor local (on premise) amb la solució ePO del mateix fabricant.

Addicionalment, el CSdM va realitzar un estudi i proves de concepte (PoC) de les solucions EDR líders en el mercat i es va decidir fer un pilot amb la solució de SentinelOne en un 10% de les estacions de treball i un 50% dels servidors del CSdM. Aquest pilot inclou serveis de SOC ofert per un partner autoritzat pel fabricant per disposar d'una servei gestionat de detecció i resposta d'amenaces de seguretat avançades, també conegut com a MDR.

4 REQUERIMENTS TÈCNICS

4.1 Descripció

Inclou el subministrament, configuració i posada en marxa d'una solució EDR amb un servei de SOC totalment gestionat. En els següents apartats es detallen els requeriments que ha de complir l'empresa adjudicatària en la seva oferta.

4.2 Requisits de la solució requerida

La solució proposada ha de complir:

1. Agent únic per actiu.
2. Agent compatible amb sistemes Windows, Linux i Mac.

3. Disposar d'un agent compatible amb versions legacy de sistemes operatius (mínim Windows XP SP3 i Windows Server 2003 R2 SP2).
4. Funcionament autònom de l'agent, amb o sense connexió a Internet.
5. Capacitat de detecció en temps real de malware basat en signatures i malware desconegut "zero day" (basat en comportament). Inclòs malware que s'executa en memòria (sense ús de fitxers).
6. Mapeig i correlació de tècniques d'atacs segons el estàndard de la matriu de classificació MITRE que faciliti el anàlisis forense.
7. Capacitat per contenir de manera automàtica incidents, bloquejant processos malintencionats, posant en quarantena fitxers o aïllant els equips afectats, per evitar la seva evolució i propagació.
8. Capacitat per definir llistes negres i blanques personalitzades, utilitzant exclusions.
9. Capacitat de fer exclusions per hash (en format SHA1 o SHA256), path, nom de fitxer o tipus de fitxer. Aquestes es podran aplicar a un grup d'equips o aquells que tinguin una determinada etiqueta (tag).
10. Disposar d'un catàleg d'exclusions agrupades per nom d'aplicació, que permeti aplicar totes les excepcions conegudes d'una determinada aplicació.
11. Disposar d'un desktop Firewall per Windows, Linux i Mac i una gestió centralitzada al cloud de les polítiques locals dels equips.
12. Capacitat per fer rollback amb un clic per sistemes operatius Windows. En cas d'infecció d'un dispositiu, es podrà fer una recuperació automàtica del sistema i arxius de l'equip afectat a un punt anterior a la infecció.
13. Disposar d'una API amb totes les funcionalitats disponibles: capacitat d'orquestrar accions de la interfície gràfica de la consola de gestió des de altres aplicacions fent ús de la API, per poder-se integrar amb solucions de tercers.
14. Control de dispositius USB i bluetooth. Que permeti denegar accés, permetre només la lectura i permetre lectura i escriptura.
15. **Retenció de registres d'activitat** dels equips, per un posterior anàlisis forense i *threat hunting*, durant un **mínim de 90 dies per servidors i un mínim de 14 dies per estacions client** (emmagatzemament en cloud).
16. Disposar d'una Storyline per visualitzar com s'ha produït i evolucionat un incident de seguretat.
17. Auditoria d'activitat dels usuaris de la consola registrada amb possibilitat d'enviament a un repositori de log extern (SIEM).
18. Connector natiu amb el SIEM Splunk, disponible en la seva Marketplace, per la integració amb el SIEM de l'Agencia de Ciberseguretat de Catalunya.
19. Creació d'alertes personalitzades.
20. Inventariat d'actius i d'aplicacions.

21. Capacitat per identificar altres dispositius connectats a la xarxa (no protegits per la solució) i realitzar polítiques d'aïllament d'aquests equips a través del propi agent instal·lat.
22. Diferents perfils d'accés a la consola: segregació d'administradors, operadors i usuaris de consulta.
23. Flexibilitat en la creació de jerarquies de polítiques de protecció.
24. Manteniment del nivell de protecció en cas de desconnexió de l'agent amb la consola cloud.
25. Capacitats anti-tamper, per evitar que la protecció sigui des-instal·lada o desactivada, inclòs amb privilegis d'administrador, i que les Shadow Copies de Windows resultin compromeses.
26. Informació en emmagatzemada en local i en repositori cloud encriptada.
27. Gestió d'actualitzacions esglaonada o per lots des de la consola, per evitar col·lapsar la xarxa.
28. Eliminació automàtica opcional dels agents d'equips que fa temps no comuniquen.
29. Desinstal·lació automàtica i desatesa dels agents des de la consola a partir de polítiques.
30. Gestió de vulnerabilitats i correlació del software instal·lat amb les vulnerabilitats (CVEs) de MITRE.
31. Consola privada per al client i servei de SOC ofert pel partner oficial en infraestructura SaaS del fabricant de la solució.
32. L'accés a la consola de gestió haurà de disposar d'un doble factor d'autenticació i aquest haurà de ser obligatori per tots els usuaris que hi tenen accés.
33. La consola de gestió haurà de ser única tant per servidors com estacions de treball.
34. La consola de gestió ha de permetre la obertura d'una Shell remota completa contra els equips. L'accés ha d'estar securitzat mitjançant doble factor d'autenticació i les accions han de quedar registrades en l'auditoria.
35. La consola de gestió s'ha d'oferir en modalitat software com a servei (SaaS), accessible des de Internet amb navegadors estàndards, sense infraestructura hardware local, evitant la necessitat d'instal·lar servidors locals a les dependències del client.
36. La comunicació entre els agents i la consola cloud seran sempre xifrats amb mètodes robustos i seguretat contrastada
37. Gestió d'actualització d'agents en base a la estructura de AD i amb possibilitats de gestionar les descàrregues simultànies.
38. La solució ha de reportar, sense configuració addicional, els atributs de ActiveDirectory (AD) registrats en l'equip (usuari, domini, DN, memberOf, etc).
39. La solució ha de permetre agrupar de forma dinàmica els actius en funció dels atributs de AD.
40. La solució ha permetre aplicar polítiques segons atributs de AD.

41. La solució ha de permetre/bloquejar comunicacions externes o internes fent ús del Desktop Firewall. Ha de suportar el filtre per FQDN, IP, CIDR, rangs d'IPs, aplicacions, ports, protocol, etc.
42. La solució ha de permetre la creació de dashboards dinàmics, dins de la mateixa consola de gestió, que mostrin la següent informació:
    a. Detecció per tipologia de motor de detecció en un període de temps concret.
    b. Versions dels agents desplegats.
    c. Agents que requereixen una acció addicional.
    d. Agents per sistema operatiu.
    e. Agents connectats i no connectats a la consola.
43. La solució ha de figurar en el quadrant de lideres del "Magic Quadrant for Endpoint Protection Platforms" de Gartner més recent (Juliol 2024).
44. La solució ha de presentar alta taxa de detecció única igual o superior al 90% en la avaluació de MITRE ATT&CK Engenuity de 2024 (Enterprise), sense requerir canvis de configuració de la solució.
45. La solució ha de disposar de qualificació vigent per catàleg CPSTIC del CCN-CERT, de la família EDR, amb categoria ENS MEDIA o superior.
46. Els serveis de gestió proposats pel licitador haurà de comptar amb presència física dins del territori espanyol.
47. El servei haurà de comptar amb funcionalitats de SOC en modalitat 24x7x365 amb al menys dos nivells de personal.
48. El servei haurà d'incloure intel·ligència d'amenaces amb definició d'indicadors de compromís (IOC), indicadors d'atac i un pla de millora continua (retroalimentació).
49. El SOC del licitador haurà d'estar connectat homologat en la Red Nacional de SOCs del CCN CERT.
50. Incloure un servei 24x7x365 de reforç al SOC del licitador prestat per personal del fabricant expert de la solució EDR.

Els **serveis professionals** necessaris per la configuració i posta en marxa de la solució proposades poden consultar a l'apartat "**4.3 Descripció detallada dels serveis**".

Caldrà una descripció detallada del disseny de la solució que doni resposta aquests requeriments, així com dels elements que la composen.

Per tal comprovar el compliment dels darrers punts de requeriments mínims d'obligat compliment, els licitadors hauran de complimentar l'ANNEX 1 amb la corresponent justificació que ho acrediti.

4.3 Descripció detallada dels serveis

L'empresa adjudicatària haurà d'incloure a la seva oferta tots els serveis que permetin completar les activitats necessàries que garanteixin l'èxit de la implantació de la solució, que inclogui:

1. Els serveis de **preparació,** incloent les tasques prèvies necessàries per assegurar una

implantació correcta de la solució, sobretot en l'àmbit de servidors, com ara comprovacions del disseny d'infraestructura actual, connectivitat, programari instal·lat en els equips), **i subministrament** del programari ofert en la licitació**.**

2. Els serveis d' **instal·lació, configuració, proves i posada en producció** del programari proposat. Aquesta tasca es podrà realitzar dins de l'horari laboral.

   Concretament els serveis inclosos han de contemplar:

   - **Desplegament de l'agent (estació client)**. El licitador proporcionarà un paquet d'instal·lació a l'àrea IT del client. Aquest paquet consistirà en l'agent a instal·lar als actius a protegir, juntament amb un manual d'instruccions per dur a terme la instal·lació i configuració del mateix de forma centralitzada i desatesa. L'oferent haurà de donar el suport corresponent davant de qualsevol problema o incidència que sorgeixi a la instal·lació, durant la fase de desplegament d'agents.
   - **Desplegament de l'agent (servidors):** El licitador realitzarà la instal·lació manual de l'agent amb les màximes garanties per tal de reduir el risc i l'impacte d'un tall de servei o comportament no desitjat. Analitzat les característiques de cada servidor, per si cal ampliació de recursos, i el programari instal·lat, per tal d'afegir prèviament les excepcions d'interoperabilitat recomanades.
   - **Desplegament consola de gestió:** El licitador realitzarà el desplegament de la consola de gestió en infraestructura cloud del fabricant de la solució EDR. S'encarregarà de realitzar el disseny, configuració i aplicació de polítiques de seguretat i d'actualitzacions dels agents.
   - **Integració amb el SIEM de l'Agencia de Ciberseguretat de Catalunya (ACC):** El licitador donarà suport a l'ACC per realitzar la integració amb el seu SIEM (Splunk).

3. **Formació** als tècnics que el CSdM designi per a l'operació i l'administració mínima del sistema, en cas que es requereixi. A la proposta de l'empresa s'haurà d'especificar el plantejament i el contingut de la formació així com el número d'hores compromeses per impartir aquesta formació (un mínim 8 hores en format remot).

4. El **servei de SOC** haurà d'incloure les següents activitats:

   - Detecció:
     - Supervisió, correlació i priorització d'alertes les 24 hores del dia, els 7 dies de la setmana.
     - Monitorització continua del entorn del client en busca d'indicadors de compromís (IoC) o indicadors d'atac IoA) recents.
   - Investigació:
     - Generació d'un anàlisis de causa per identificar el vector d'atac, el temps de permanència, mètode de propagació i impacte de l'atac.
     - El client podrà treballar directament amb els analistes de seguretat durant aquest procés d'investigació per decidir la millor resposta.
   - Resposta:
     - Accions de resposta automàtiques o manuals i per contenir amenaces i generar IoC per prevenir futurs atacs. Recomanacions para mitigar, contenir, remeiar o eradicar l'amenaça.
     - Notificar sempre al client sobre un incident de seguretat a través del mètode pactat.
   - Informes:
     - Report mensual que descrigui els serveis prestats durant el període de temps especificat, incloent informació sobre:

- Resum de l'estat dels elements protegits dins l'abast del contracte.
- Llistat d'incidents de seguretat detectats, incloent-hi resum d'intents d'atac per tipologia d'amenaça i detecció.
- IoC detectats i bloquejats
- Nivells aconseguits de SLA.

- **Actualitzacions de l'agent**: L'adjudicatari, com a part del servei gestionat, serà l'encarregat d'actualitzar els agents instal·lats durant la vigència del contracte, seguint un pla que minimitzi el possible impacte de les accions requerides. Es farà des de la consola de gestió cloud sense intervenció de Client tret que sorgeixi un problema. Aquesta actualització serà consensuada amb el Client i programada a les finestres que autoritzi el Client.

- **Reinici d'agents en cas de pèrdua de connectivitat**: En cas de detectar-se una pèrdua de connectivitat del servei amb l'agent d'EDR, es contactarà amb el personal del Client o el proveïdor de IT que administri i operi els equips per indicar-li el procediment per recuperar la connectivitat. Si es tracta d'un problema recurrent, el licitador haurà d'indicar una acció correctiva que solucioni el problema de forma permanent.

Addicionalment i de forma puntual:

- L'adjudicatari facilitarà un manual d'instruccions al Client i/o al seu proveïdor de IT que administri i operi els servidors perquè configurin la monitorització d'aquest agent a nivell de servei a la plataforma de monitorització corresponent (Nagios XI). Addicionalment des del servei gestionat del SOC (Managed EDR) es realitzarà una monitorització de la connexió i funcionament d'aquest agent amb la Consola.

5. Servei de **bossa d'hores:**

   - L'adjudicatari posarà a disposició del client, una bossa de **50 d'hores** per atendre exclusivament els següents supòsits:

     a. Incidents de cibserseguretat que requereixin recursos humans addicionals al equip de IT existent per la ràpida i efectiva resposta.

     b. Suport a l'equip IT local en el cas de futurs desplegaments de l'agent que requereixin un anàlisis previ de les característiques i programari de l'equip per realitzar la instal·lació amb les màximes garanties per tal de reduir el risc i l'impacte d'un tall de servei o comportament no desitjat.

   NOTA: CSdM no s'obliga a consumir la partida de la bossa d'hores, per tant només es facturarà el que s'hagi executat i aprovat prèviament per ambdues parts.

Totes les operacions i despeses relacionades amb els serveis descrits seran a càrrec de l'adjudicatari. En cap cas s'acceptaran càrrecs addicionals a l'oferta econòmica presentada i adjudicada.

4.4 Garantia del subministrament

La garantia del subministrament comprèn el suport i manteniment definit en aquest plec..

Un cop executada la posada en marxa de l'equipament i/o programari, i quan s'hagi signat la

corresponent acta de recepció, tots els elements (maquinari i programari) de la solució s'han d'incloure dins la garantia contractual el suport i manteniment, en compliment d'aquest plec tècnic.

5 CONDICIONS DE LLIURAMENT

5.1 Condicions de lliurament i calendari (SOBRE B)

El termini de lliurament del programari i serveis proposats quedarà inclòs dins del termini d'execució (veure punt 2.3 del present plec).

5.2 Transport, embalatge i residus

El transport de l'equipament fins al seu punt final d'utilització anirà a càrrec de l'empresa adjudicatària.

Els equipaments hauran d'anar convenientment embalats per tal que arribin en les millors condicions. Qualsevol desperfecte dels materials ocasionat en el transport fins el punt d'utilització anirà a càrrec de l'empresa proveïdora.

El desembalatge i recollida de residus generats durant el desembalatge i instal·lació de l'equipament aniran a càrrec de l'adjudicatari. L'adjudicatari retirarà els residus del centre i en farà un tractament d'acord a la legislació vigent.

5.3 Requisits a complir per part de l'adjudicatari

És obligació expressa de l'adjudicatari la no subcontractació dels serveis objecte del contracte a altres empreses, atès que totes les tasques que el comprenen es consideren tasques crítiques i les característiques de l'empresa adjudicatària han estat determinants en l'adjudicació al seu favor.

Per a cadascun dels equipaments oferts, el licitador demostrarà el compliment de la legislació vigent i la normativa d'obligat compliment relativa a l'equip amb el certificat corresponent al **compliment de la marca CE** per a l'equip ofert, en marca i model pertinent.

Serà responsabilitat del contractista el compliment de la normativa legal de caràcter tècnic, administratiu, laboral i de seguretat i higiene, actualment en vigor, així com les que es dictin durant el transcurs del contracte.

D'altra banda seran d'obligat compliment les normatives que estableixi el centre per raons de funcionalitat i/ o asèpsia, i d'acord a les característiques de la pràctica hospitalària i amb el respecte degut al pacient.

L'empresa adjudicatària de l'equipament disposarà del **propi pla de seguretat i salut** per a la instal·lació dels equips en els termes que la normativa vigent estableixi, per tots els treballs auxiliar derivats de l'abast del contracte.

6 GOVERNABILITAT DEL PROJECTE

Caldrà identificar en l'oferta que presentin els licitadors els perfils tècnics i no tècnics que participin en el transcurs del contracte. El número de recursos assignats per la realització dels serveis descrits anteriorment serà el que l'empresa adjudicatària estimi necessaris per complir amb les necessitats indicades.

S'haurà de fer una proposta de governabilitat i d'execució dels serveis, on com a mínim quedin definits els següents perfils mínims:

- **Director del servei**: responsable del servei per part de l'adjudicatari davant del client. S'encarregarà d'organitzar i reservar els recursos necessaris dintre de l'empresa per la correcta prestació del servei. Supervisar el compliment dels nivells de servei (SLAs). Participarà en les reunions de seguiment i validarà i presentarà els informes del serveis prestats.
- **Responsable tècnic**: supervisarà i gestionarà la resolució de les incidències de major gravetat, es a dir, aquelles que afectin a equips més crítics o tinguin major impacte per la infraestructura del client. Identificarà i donarà resposta a les necessitats del client i identificarà i prepararà propostes de millora de la solució proposada.
- **Tècnic de suport**: atenció a les incidències generades per la solució proposada i execució de tasques d'administració, actualització i manteniment d'aquesta.

- **Comitè operatiu**: estarà integrat pel cap de projecte de l'empresa adjudicatària i els membres del CSdM que es designin. La seva funció serà la planificació, comunicació i coordinació entre membres de l'empresa proveïdora i del client, avaluació i gestió de riscos, control de qualitat, compliment normatiu, contractual i normes de seguretat. Es farà un seguiment a l'inici de la contractació, mínim quinzenalment, per revisar la proposta de planificació presentada i la seva execució. Aquest seguiment pot fer-se no presencialment. El **perfil assignat del cap de projecte** requereix que tingui la següent **certificació mínima**:
  - **ITIL Foundation**

- **Comitè tècnic**: estarà integrat pel personal tècnic de l'empresa adjudicatària i els membres del CSdM que es designin. La seva funció serà la implementació de la configuració i posta en marxa de la solució amb la màxima qualitat, així com la formació a membres tècnics del CSdM i la redacció de la documentació final de projecte. Es farà un seguiment a demanda de les necessitats del projecte, i mínim quinzenalment. Aquest seguiment pot fer-se no presencialment.
  - El **perfil tècnic** assignat a aquest projecte requereix que tingui la següent certificació mínima:
    - **Certificació tècnica de tipus professional o especialista en la solució MDR proposada.**

7 ACORDS DEL NIVELL DE SERVEI (SLA) DE LA GARANTIA/MANTENIMENT

S'entén per Acords de Nivell de Servei, el nivell de prestació exigit a l'oferent per a cadascun dels indicadors, amb l'objectiu d'establir paràmetres mesurables que permetin al CSdM, com a contractant del servei, i a l'oferent, controlar-ne la qualitat dels serveis prestats

	DESCRIPCIÓ	**SLA**
SOC MDR **Disponibilitat de la Plataforma i sistemes de notificació**	Aplicacions MDR y SOC La disponibilitat de la plataforma es mesurarà pel número total de minuts del mes, menys el número de minuts que el sistema no està disponible al mes (ajustat per qualsevol temps d'inactivitat programat) dividit pel número total de minuts al mes x 100.	99% Disponibilitat del 99% pel sistema de gestió i consola web.
Temps de resposta a incidents	Es refereix únicament a la resposta inicial d'un analista sobre un incident generat per la solució (primer anàlisis). Depenen de l'estat de l'incident (per exemple, si s'ha realitzat o no una acció de resposta automàtica)	Actiu/Sospitós: 3 hores Mitigat/Bloquejat: 5 hores
Reporting	Informes mensuals	≥ 75% de informes mensuals i els seus documents associats entregats durant els primers 15 dies de cada mes.

7.1 Penalitzacions

En cas de superar el valor del nivell de cada SLA establert, s'incorrerà en una penalització d'acord amb el següent :

	DESCRIPTION	**PENALITZACIÓ**
SOC MDR **Disponibilitat de la Plataforma i sistemes de notificació**	Aplicacions MDR y SOC La disponibilitat de la plataforma es mesurarà pel número total de minuts del mes, menys el número de minuts que el sistema no està disponible al mes (ajustat per qualsevol temps d'inactivitat programat) dividit pel número total de minuts al mes x 100.	Penalització d'un 1%, per disponibilitat entre 95-99%) i 3%, per disponibilitat inferior a 95%, en la facturació mensual en cas d'acumular dos períodes per sota del valor requerit.
Temps de resposta a incidents	Es refereix únicament a la resposta inicial d'un analista sobre un incident generat per la solució (primer anàlisis). Depenen de l'estat de l'incident (per exemple, si s'ha realitzat o no una acció de resposta automàtica)	Penalització d'un 1% de la facturació mensual en caso d'acumular dos incidents per sota del valor requerit. Penalització acumulable.
Reporting	Informes mensuals	Descompte d'un 2% de la facturació mensual del servei.

8 CONDICIONS DEL SUPORT

8.1. Contacte

L'Adjudicatari facilitarà un suport telefònic i adreça de correu electrònica als usuaris autoritzats pel CSdM per contactar amb els tècnics de suport, ja sigui per comunicar incidències que hagin de ser resoltes o per transmetre les consultes que considerin oportunes durant la fase d'execució i garantia d'aquesta licitació.

8.2. Assistència presencial

Totes les intervencions cobertes per la garantia i suport s'executaran, per defecte, mitjançant accés remot segur (VPN+MFA) des del SOC de l'adjudicatari.

El CSdM podrà exigir desplaçament in situ quan concorri, almenys, una de les següents circumstàncies:

a) L'actiu afectat no té connectivitat amb la consola EDR o l'agent no s'està executant.

b) La resolució requereix manipulació física (desconnexió de xarxa, anàlisi forense).

En aquests casos, l'adjudicatari aportarà el personal habilitat, l'equipament i les EPI necessàries, assumint les despeses de desplaçament.

8.3. Infraestructura necessària per a dur a terme el suport

El lloc de treball han de ser les instal·lacions que estableixi l'adjudicatari (en cap cas seran les instal·lacions del Consorci Sanitari del Maresme a menys que hi hagi una petició expressa del propi Consorci Sanitari del Maresme).
L'equip responsable per part del proveïdor per realitzar el suport descrit en aquesta licitació disposarà de les eines de connexió remota (VPN) amb la infraestructura del client, cosa que ajuda a evitar desplaçaments als tècnics de suport i a obtenir millor resposta en cas d'incidència o necessitat.

9 DOCUMENTACIÓ TÈCNICA A APORTAR PELS LICITADORS (SOBRE C)

Cal presentar l'oferta de forma estructurada i breu, evitant informació comercial que no sigui imprescindible. El licitador haurà de respectar en tot moment les pautes i condicions establertes.

El paginat màxim de l'oferta serà de 50 pàgines en total, i presentades en un ÚNIC ARXIU PDF, amb totes les pàgines numerades de forma correlativa i seguint l'índex corresponent i amb tipus de **lletra Arial 10**.

Los ofertes hauran de donar resposta a les demandes plantejades en aquest Plec de Prescripcions Tècniques, descrivint el detall dels servei, segons aquesta proposta d'**ÍNDEX**:

1. **Requisits imprescindibles**:
   - Complimentar **fitxer Annex 1- Justificació requeriments mínims**, segons indicacions punt 11 Documentació requisits mínims.

     En cas que ho consideri convenient, l'equip avaluador de la licitació pot sol·licitar als licitadors demostracions de la solució proposada a fi de poder validar el compliment dels requeriments tècnics mínims descrits en el present plec. L'empresa està obligada a facilitar aquesta demostració en el termini màxim d'una setmana des que és requerida.
2. Descripció del **disseny de la solució i de tot l' equipament** que el licitador presenta en l'oferta tècnica amb les seves especificacions tècniques i funcionals. Dintre de la proposta tècnica s'ha d'incorporar els catàlegs tècnics i/o referències i/o documentació necessària per la correcta justificació del compliments dels punts especificats en aquest document.
3. Descripció de la proposta d' execució:
   3.1. **Cronograma detallat** que contempli totes les activitats necessàries i les seves interrelacions per donar compliment aquest PPT (tasques de preparació, terminis de lliurament, configuració, i posada en marxa...)
   3.2. **Descripció detallada de la proposta de tasques de preparació i subministrament** del material i/o servei ofert en la licitació.
4. **Descripció detallada de la proposta de Formació** als tècnics de CSdM.
5. **Descripció detallada del suport i garantia/manteniment**.
6. **Descripció de la Governança del projecte**: Descripció de **l'equip de treball**, identificant el perfil tècnic que participarà en cadascuna de les fites del projecte, així com la figura de cap de projecte.

IMPORTANT:

- ***No aportar els certificats i documentació anteriorment descrits, implicarà l'exclusió de la present licitació.***
- ***La informació que no estigui recollida amb la numeració sol•licitada, el paginat descrit, i amb l'índex indicat, no serà llegida ni valorada***

10 DOCUMENTACIÓ ECONÒMICA (SOBRE C) A APORTAR PELS LICITADORS

Les ofertes hauran d' **emplenar l'Annex OE - Valoració Objectiva,** on es demana la **valoració econòmica** de la proposta amb un import **màxim** estimat de **315.600 € (sense IVA) pel període de 3 anys.**

11 DOCUMENTACIÓ JUSTIFICACIÓ REQUERIMENTS MÍNIMS

En un fitxer adjunt es facilita aquest annex (**Annex 1- Justificació requeriments mínims**) que caldrà emplenar i incloure en el **sobre C**, per facilitar l'avaluació del compliment de les característiques tècniques mínimes obligatòries, o requeriments.

Cal indicar en cada punt si es compleix amb el requisit i el detall del compliment en format breu a la columna Justificació. Per tal de poder fer la comprovació d'aquesta informació, caldrà detallar també la següent informació en els punts on es requereixi:

- Pàgina de l'oferta on s'explicita el requeriment o enllaç a la documentació oficial en línia o document de dades del producte (o datasheet), que acrediti el compliment del requeriment.
- En cas de no existir cap document oficial dels esmentats al punt anterior, o de faltar alguna dada a acreditar requerida, caldrà incorporar un certificat oficial del fabricant de l'element on es confirmi que es compleix el punt descrit a l'apartat de requeriments.

Veure fitxer Annex 1 – Justificació requeriments mínims

ID.	Requisit	Compleix (SI o NO)	Breu justificació (1)	Indicar la pàgina on poder confirmar la informació (1)(2)

on

(1) Si en un mateix document es cobreixen tots els aspectes de l'element en qüestió, no cal referenciar-lo a cada fila/requisit, es pot indicar el número de la primera fila que el conté.

(2) Pàgina de la oferta on s'explicita o enllaç a documentació oficial o certificat del fabricant