

Codi de verificació:	 5G12495N3726143S14IG
Procediment: N488 Contractació de serveis	
Expedient: 17295/2025	Document: 405500/2025

MEMÒRIA JUSTIFICATIVA DEL CONTRACTE

De conformitat amb els articles 28, 100, 101 i 116.4 de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic (en endavant, LCSP), s'emet aquesta memòria justificativa del contracte

Àmbit de gestió: Tecnologia

Servei: Servei de Tecnologia i Desenvolupament Digital

Denominació del contracte: Servei Gestionat de Ciberseguretat (MSSP)

A. Objecte del contracte

L'Ajuntament de Sant Cugat del Vallès té la responsabilitat ètica i legal de garantir la seguretat dels seus sistemes d'informació i la protecció de les dades que gestiona. Això implica assegurar que el tractament de dades es realitza en entorns tecnològics segurs, robustos i eficients.

La **seguretat de la informació** és un servei essencial per al bon funcionament de l'Ajuntament, especialment en la seva dimensió estratègica. Una gestió eficaç de la ciberseguretat reforça la confiança ciutadana i millora la qualitat de la gestió pública.

Actualment, l'Ajuntament presenta certes limitacions en la seva capacitat de resposta ràpida davant incidents de seguretat, fet que augmenta el risc d'impactes greus. Segons dades del **CCN-CERT**, durant el 2023 es van registrar més de 100.000 incidents a nivell estatal, amb un increment superior al 20% respecte a l'any anterior. D'aquests, més del 15% van ser classificats com a crítics o d'altíssima gravetat.

Entre les amenaces més rellevants es troben:

- **Ciberatacs impulsats per actors estatals**, amb objectius de desinformació i influència política.
- **Ciberdelinqüència econòmica sofisticada**, com el frau del CEO o el ransomware operat per humans.
- **Atacs a sistemes ciberfísics**, tant directes com per danys col·laterals.
- **Explotació de vulnerabilitats en sistemes exposats a Internet**, agreujada pel teletreball.

- **Increment de regulacions i normatives** en matèria de ciberseguretat, que exigeixen més compliment i control.
- **Ús creixent de la intel·ligència artificial** tant per part d'atacants com de defensors.
- **Riscos derivats d'un ús inadequat de la IA**, com deepfakes, automatització d'atacs, biaixos algorítmics o manipulació de dades.

Amb aquest context, l'Ajuntament impulsa una licitació per contractar **solucions i serveis de ciberseguretat** que responguin a les necessitats actuals. L'objectiu és disposar d'un **servei unificat** que combini:

- Capacitats avançades de **correlació i gestió d'esdeveniments de seguretat (SIEM)**.
- Funcionalitats d'**orquestració i automatització de respostes (SOAR)**.
- **Gestió i resposta** a incidents de seguretat.
- **Gestió del risc i la superfície** d'atac de l'organització.
- **Aplicacions d'intel·ligència artificial** per millorar la detecció, anàlisi i resposta davant incidents complexos.

Aquest servei ha de garantir una **protecció integral i robusta** dels sistemes d'informació municipals.

Justificació de la manca de mitjans de l'Ajuntament per satisfer les necessitats:

L'Ajuntament de Sant Cugat del Vallès no disposa de mitjans ni personals ni materials propis adients per a la realització d'aquests treballs, atesa la complexitat tècnica i especialització que requereix actualment la gestió efectiva de la ciberseguretat. L'evolució ràpida i contínua de les amenaces digitals, juntament amb la necessitat d'implementar tecnologies avançades com la intel·ligència artificial per a la detecció proactiva i la resposta immediata, exigeix uns recursos especialitzats que superen àmpliament les capacitats actuals de personal i infraestructura pròpies.

A més, la dotació existent en matèria de seguretat informàtica de l'Ajuntament es veu limitada en aspectes essencials com la disponibilitat de personal expert en ciberseguretat, eines avançades de monitorització contínua i resposta ràpida davant d'incidents. Aquestes limitacions fan imprescindible la contractació externa de serveis altament especialitzats per assegurar el nivell adequat de protecció i resposta davant d'amenaces creixents i cada vegada més sofisticades.

Contracte de serveis que comporta prestacions directes a favor de la ciutadania, de conformitat amb l'article 312 de la LCSP: Sí ☐ No ☒

· Data d'aprovació de l'establiment del règim jurídic del servei:

Codi CPV i descripció

72500000-0 Serveis informàtics

Divisió en lots: Sí ☐ No ☒

No escau la divisió en lots d'aquest contracte, atès que la naturalesa dels serveis inclosos en el seu objecte implica una estreta interrelació i coordinació que fa inviable executar-los de manera independent, i això impossibilitaria el correcte desenvolupament global del projecte, d'acord amb el que estableix l'article 99.3.b) de la LCSP.

El contracte comprèn un conjunt integrat de serveis que cal desenvolupar, planificar i coordinar conjuntament i de forma coherent en el temps, fent que una divisió en prestacions individuals no permeti assolir els objectius previstos ni generar cap aprofitament per separat.

Contractació reservada a centres especials de treball o a empreses d'inserció, de conformitat amb la disposició addicional quarta de la LCSP: Sí ☐ No ☒

Limitacions en l'adjudicació de lots: Sí ☐ No ☒

B. Termini de vigència del contracte

B1. Vigència inicial del contracte: El contracte tindrà una durada inicial de 2 anys a comptar des de la data que es determini en l'acta d'inici de la prestació del servei. (previsió Dic 25 – Nov 27)

B2. Prorrogable ☒ Sí ☐ No

El contracte podrà ser prorrogat fins a un màxim de 2 anualitats addicionals.

B3. Terminis d'execució parcial: ☒ Sí ☐ No

Els terminis d'execució parcials es determinen en el PPT.

C. Dades econòmiques

C1. Determinació del preu:

☐ A tant alçat

☐ Preus unitaris i unitats certes

☐ Preus unitaris i pressupost màxim estimatiu vist que les unitats són estimades, d'acord amb les previsions de la disposició addicional 33a de la LCSP

☒ Pressupost màxim estimatiu vist que el preu total del contracte inclourà una part fixa determinada per preus unitaris i una part variable determinada per preus unitaris:

- La part fixa, que correspon a les següents prestacions: totes les prestacions definides al plec de prescripcions tècniques i que no fan referencia a la part variable.
- La part variable, a realitzar en funció de les necessitats de l'Ajuntament, que correspon a les següents prestacions: En aquest sentit, la part variable prevista en aquesta licitació està orientada a cobrir tasques derivades de recomanacions específiques fetes per equips especialitzats com són:
 - **DFIR (Resposta i Anàlisi Forense Digital):** Pot recomanar actuacions addicionals després d'investigar incidents de seguretat per tal de reforçar les defenses o minimitzar riscos futurs.
 - **CSIRT (Equip de Resposta davant Incidents):** És habitual que, després d'analitzar alertes o incidents, suggereixi implementacions puntuals o ajustos per augmentar la capacitat de resposta i reduir la superfície d'atac.
 - **Security Manager (interlocutor únic de seguretat):** En el marc del seu seguiment continu, pot identificar àrees de millora en la gestió de la seguretat i proposar accions concretes que no eren previsibles inicialment però que són crítiques per garantir la protecció adequada dels sistemes.

Igualment, aquesta part variable també permet incorporar la implantació de tecnologies específiques recomanades per aquests equips, orientades exclusivament a millorar la seguretat global de l'organització davant de riscos emergents.

C2. Pressupost base de licitació:

De conformitat amb l'article 100 de la LCSP, el pressupost base de licitació d'aquest contracte és el que es detalla a continuació i la justificació del seu càlcul consta en l'**annex 1** d'aquesta memòria justificativa del contracte:

Part fixa	Import anual	Import total (2 anys de contracte)
Preu base de licitació	157.793,60 €	315.587,20 €
IVA (21%)	33.136,66 €	66.273,31 €
Total	190.930,26 €	381.860,51 €

Part variable	Import anual	Import total (2 anys de contracte)
Preu base de licitació	14.470,00 €	28.940,00 €
IVA (21%)	3.038,70 €	6.077,40 €
Total	17.508,70 €	35.017,40 €

Total part fixa + part variable	Import anual	Import total (2 anys de contracte)
Preu base de licitació	172.263,60 €	344.527,20 €
IVA (21%)	36.175,36 €	72.350,71 €
Total	208.438,96 €	416.877,91 €

C3. Valor estimat del contracte (VEC) i mètode aplicat per al seu càlcul:

D'acord amb les previsions de l'article 101.5 de la LCSP, pel càlcul d'aquesta quantia s'ha tingut en compte l'import del pressupost base de licitació (IVA exclòs), així com també, si s'escau, la possibilitat i imports de les potencials pròrrogues i modificacions previstes en aquest plec d'acord amb les previsions de l'article 204 de la LCSP.

Import període inicial del contracte	344.527,20 €
Import modificacions	68.905,44 €
Import pròrrogues	344.527,20 €
Import modificacions a les pròrrogues	68.905,44 €
Total valor estimat del contracte (IVA Exclòs)	826.865,28 €

La justificació del càlcul del valor estimat, consta en l'**annex 1** d'aquesta memòria justificativa del contracte.

D. Modificacions previstes del contracte

De conformitat amb l'article 204 de la LCSP, aquest contracte podrà ser modificat per les següents causes. Aquestes modificacions podran comportar una alteració del preu del contracte, a l'alça o a la baixa, fins a un màxim del 20% del seu import.

Causas de modificació previstes:

- **Descripció de la modificació:** Aquestes modificacions es justifiquen especialment per la naturalesa dinàmica i canviant de la ciberseguretat, i poden respondre a situacions com ara:
- **Canvis en el nombre de fonts de logs:** pot ser necessari ampliar o reduir les fonts d'informació integrades en la plataforma per ajustar-se a les necessitats reals de seguretat que es vagin detectant durant la prestació del servei.
- **Tasques derivades de recomanacions especialitzades:** ajustos que siguin requerits per part dels equips especialitzats com el SOC (Centre d'Operacions de Seguretat), el CSIRT (Equip de Resposta a Incidents de Seguretat), DFIR (Resposta i Anàlisi Forense Digital) o l'interlocutor únic (Security Manager), que sovint proposaran millores

derivades d'anàlisis tècniques, auditories o incidents detectats durant l'explotació del servei.

- **Adaptació a canvis normatius o legislatius futurs:** l'aparició de noves normatives o requisits legals posteriors a l'elaboració d'aquesta licitació poden exigir modificacions per complir obligacions que encara no existeixen o que no es poden preveure amb precisió en l'actualitat. Un exemple clar és la implantació de solucions exigides pel Reial Decret 311/2022, o qualsevol altra normativa posterior.
- **Assessorament tècnic especialitzat fora de l'objecte inicial:** en determinats casos podria ser necessari contractar serveis puntuals d'assessoria tècnica experta sobre aspectes específics de ciberseguretat, no contemplats inicialment però imprescindibles per garantir o millorar el nivell de protecció.
- **Incorporació i suport de noves tecnologies no previstes inicialment:** donada la ràpida evolució tecnològica en l'àmbit de la ciberseguretat, és molt probable que durant la durada del contracte sigui necessària la implementació, integració o suport a noves tecnologies, eines o plataformes que encara no existeixen o que no s'han contemplat en el moment de redactar aquesta licitació. Aquesta flexibilitat és fonamental per garantir la capacitat d'adaptació als nous riscos i amenaces que puguin aparèixer durant el període contractual.

E. Existència de crèdit

E1. Aplicació pressupostària:

La partida d'inversions és 15401 92000 6410000 Administració general/Despeses aplicacions informàtiques

Projecte 2025 / 2 / ESC02 / 1

Total	2026
Preu base de licitació	131.494,67 €
IVA (21%)	27.613,88 €
Total	159.108,55 €

Part variable	2026
Preu base de licitació	14.470,00 €
IVA (21%)	3.038,70 €
Total	17.508,70 €

La partida de manteniment és 15401 92000 2279900 Administració general/Altres treballs empres. i prof

Total	OCT - NOV 26	2027
Preu base de licitació	26.298,93 €	157.793,60 €
IVA (21%)	5.522,78 €	33.136,66 €
Total	31.821,71 €	190.930,26 €

Part variable	2027
Preu base de licitació	14.470,00 €
IVA (21%)	3.038,70 €
Total	17.508,70 €

E2. Tipologia de contractació:

Contractació anticipada (el contracte es preveu que s'iniciï a la següent anualitat):

- ☒ Sí
☐ No

Es tracta d'una licitació avançada condicionada al canvi de finançament de venda patrimonial a endeutament.

Contractació amb una subvenció vinculada:

- ☐ Sí , identificació:
☒ No

Contractació vinculada a fons europeus:

- ☐ Sí
☒ No

Contractació d'abast pluriennal:

- ☒ Sí
☐ No

E3. Distribució pressupostària de la despesa d'un expedient d'abast pluriennal:

Total	Any 1	Any 2
Preu base de licitació	172.263,60 €	172.263,60 €
IVA (21%)	36.175,36 €	36.175,36 €
Total	208.438,96 €	208.438,96 €

F. Variants

- ☐ Sí ☒ No

Elements:

Condicions:

G. Tramitació de l'expedient i procediment d'adjudicació

G1. Forma de tramitació:

- ☒ Ordinària
☐ Urgent

G2. Procediment d'adjudicació:

☐ **Procediment obert simplificat abreujat** atès que es tracta d'un contracte de serveis amb un valor estimat del contracte inferior a 60.000,00€ i que no té per objecte prestacions de caràcter intel·lectual.

☐ **Procediment obert simplificat** atès que es tracta d'un contracte de serveis amb un valor estimat del contracte inferior a 143.000 € (IVA exclòs).

☐ **Procediment obert per a l'adjudicació d'un contracte de serveis NO subjecte a regulació harmonitzada**, atès que es tracta d'un contracte amb un valor estimat del contracte no és superior a 221.000 € (IVA exclòs)

☒ **Procediment obert per a l'adjudicació d'un contracte de serveis subjecte a regulació harmonitzada**, atès que es tracta d'un contracte amb un valor estimat igual o superior a 221.000 € (IVA exclòs)

(*) Excepcions:

(*) En cas de contractes que tinguin per objecte serveis socials i/o serveis enumerats a l'annex IV de la LCSP:

☐ **Procediment obert per a l'adjudicació d'un contracte NO subjecte a regulació harmonitzada**, atès que és un contracte de serveis que el seu valor estimat (VEC) no és superior a 750.000 € (IVA exclòs)

☐ **Procediment obert per a l'adjudicació d'un contracte subjecte a regulació harmonitzada**, atès que és un contracte de serveis que el seu valor estimat (VEC) és igual o superior a 750.000 € (IVA exclòs)

(*) En cas de contractes que tinguin per objecte serveis especificats a l'article 19.2 de la LCSP:

☐ **Procediment obert per a l'adjudicació d'un contracte NO subjecte a regulació harmonitzada**, atès que té per objecte la contractació d'un dels serveis enumerats a l'article [19.2 de la LCSP](#)

H. Classificació empresarial i requisits de solvència

H.1. Classificació empresarial:

☐ D'acord amb l'article 156.9 apartat b) de la LCSP, en els contractes que s'adjudiquin mitjançant **procediment obert simplificat abreujat** els licitadors no han d'acreditar la solvència econòmica i financera i tècnica o professional, en aquest sentit, no és necessari acreditar cap classificació empresarial.

☒ De conformitat amb l'article 77.1 apartat b) de la LCSP, la solvència empresarial es podrà acreditar indistintament a través de la següent classificació empresarial o bé a través dels mitjans d'acreditació de la solvència que es descriuen a l'apartat H2.¹

Grup: V

Subgrup: V5

Categoria: 4

☐ De conformitat amb l'article 77.1 apartat b) de la LCSP, com que l'objecte del present contracte no està inclòs en l'àmbit d'algun dels grups o subgrups de classificació vigents, l'acreditació de la solvència es farà a través dels mitjans d'acreditació de la solvència que es descriuen a l'apartat H2.

H.2. Criteris de solvència econòmica i financera i tècnica o professional

☐ D'acord amb l'article 156.9 apartat b) de la LCSP, en els contractes que s'adjudiquin mitjançant **procediment obert simplificat abreujat** els licitadors no han d'acreditar la solvència econòmica i financera i tècnica o professional, en aquest sentit, no es fixen criteris de solvència.

☒ A continuació s'especifiquen els requisits de solvència econòmica o financera i de solvència tècnica o professional, relatius a aquesta contractació.

L'empresa licitadora haurà de complir els requisits de solvència que s'indiquin des del MOMENT EN QUE FINALITZI EL TERMINI DE PRESENTACIÓ D'OFERTES I SUBSISTIR FINS A LA FORMALITZACIÓ DEL CONTRACTE :

Requisits de solvència econòmica i financera

D'acord amb l'article 87 de la LCSP, es considera adequat exigir la següent solvència econòmica a les empreses licitadores o professionals licitadors:

Requisits de solvència	Mitjà d'acreditació i justificació del requisit exigít
☒ Volum anual de negocis del licitador que, referit a l'any de major volum de negoci dels tres últims disponibles (en funció de les dates de constitució, o d'inici d'activitats de l'empresari i de presentació de les ofertes) haurà de ser, com a mínim:	Presentació dels comptes anuals degudament aprovats i dipositats al Registre Mercantil o registre oficial corresponent d'aquella anualitat amb major volum anual de negocis dins dels tres últims disponibles, tal i com es preveu a l'article 87.2 de la LCSP.
☒ una vegada i mitja el valor anual mitjà del	

¹ Les classificacions es determinen de conformitat amb les previsions dels [articles 37 i següents del RGLCAP](#). Si el contracte es troba dividit en lots, cal indicar la classificació per cadascun dels lots.



contracte	Es considera adequat exigir aquesta solvència atès que el llindar mínim econòmic que garanteix que les empreses estiguin capacitades per fer front als costos econòmics derivats de l'execució d'aquest servei.
-----------	---

Requisits de solvència tècnica o professional

En compliment de l'article 90 de la LCSP, es considera adequat exigir la següent solvència tècnica i professional a les empreses licitadores o professionals licitadors:

- L'empresa licitadora haurà d'acreditar de manera fefaent la seva experiència en cadascuna de les matèries següents, totes elles imprescindibles per a l'execució del contracte: **gestió de Centres d'Operacions de Seguretat (SOC) o serveis equivalents, Equips de Resposta a Incidentes de Seguretat Informàtica (CSIRT), serveis especialitzats de Resposta i Anàlisi Forense Digital (DFIR) i serveis gestionats de seguretat (MSSP).**

Es consideraran com a serveis similars aquells que incloguin la implantació i la gestió operativa d'un Centre d'Operacions de Seguretat (SOC), serveis de resposta davant incidents (CSIRT), serveis de resposta i anàlisi forense digital (DFIR), o serveis gestionats de seguretat (MSSP).

A aquests efectes, la licitadora haurà de presentar una relació detallada dels serveis prestats durant els darrers tres anys que inclogui, de manera expressa i obligatòria per a cadascuna de les matèries esmentades:

- L'import del contracte.
- Les dates d'execució.
- La condició del destinatari (públic o privat).

L'import anual corresponent al millor exercici dels darrers tres anys haurà de ser com a mínim igual al 70% de l'annualitat mitjana establerta en aquesta licitació.

Només es consideraran serveis similars aquells que acreditin de forma explícita l'experiència en les quatre matèries indicades: SOC, CSIRT, DFIR i MSSP, essent necessari justificar-les totes per complir aquest criteri de solvència.

L'acreditació es farà de la manera següent:

- Quan els treballs hagin estat executats per Administracions públiques: mitjançant **certificats emesos per l'òrgan competent**.
- Quan els treballs hagin estat executats per entitats privades: mitjançant **certificats expedits per aquestes** o, en defecte, mitjançant una **declaració responsable de l'empresa licitadora**, acompanyada de documentació contractual que en confirmi l'execució.

Aquest criteri es fonamenta en els articles 90 i 91 de la LCSP i en l'article 16 del Reial decret 311/2022 (ENS), i és necessari i proporcionat per garantir que l'empresa adjudicatària disposa de l'experiència integral en totes les àrees crítiques de la ciberseguretat, assegurant la professionalitat i solvència indispensables per a l'èxit del servei MSSP.

- El **DataCenter**, per garantir la prestació del servei MSSP (Proveïdor de Serveis Gestionats de Seguretat) amb les màximes garanties operatives, de qualitat i seguretat,

haurà d'estar situat en territori europeu, i en cap cas podrà trobar-se fora de la Unió Europea.

Aquesta condició és imprescindible per:

- Minimitzar latències en la prestació del servei i assegurar respostes àgils davant incidents de seguretat.
- Garantir que l'operativa es realitza sota un fus horari europeu compatible amb l'Ajuntament, facilitant la coordinació immediata i evitant desajustos que podrien afectar la resposta davant incidents crítics.
- Permetre, en cas que sigui necessari, la verificació presencial de les instal·lacions per part de l'Ajuntament, com a mesura addicional de control i transparència.
- Complir amb el marc normatiu vigent, ja que:
 - El Reial decret 311/2022 (ENS) obliga a garantir la disponibilitat, integritat i confidencialitat dels sistemes i de les dades tractades pels proveïdors de serveis públics.
 - El Reglament (UE) 2016/679 (RGPD) i la LOPDGDD estableixen que les dades personals només poden ser tractades i emmagatzemades dins l'Espai Econòmic Europeu, llevat que existeixin garanties específiques reconegudes per la Comissió Europea.
 - Limitar la localització a territori europeu aporta una seguretat jurídica addicional, ja que assegura que el tractament i emmagatzematge de dades es fa sempre sota jurisdiccions alineades amb la normativa europea, evitant riscos associats a legislacions de tercers països que podrien comprometre la confidencialitat o l'accés a la informació.

El DataCenter haurà de disposar com a mínim de la certificacions:

- **TIER III** per assegurar un nivell adequat de disponibilitat i resiliència, que garanteix redundància en tots els subsistemes crítics, manteniment sense interrupcions i un nivell de servei (99,982%), així com gestionar-se d'acord amb els principals estàndards internacionals de seguretat aplicables actualment, garantint així el compliment integral de la normativa vigent.
- **ISO 27001** (Seguretat de la informació): garanteix que el DataCenter aplica controls de seguretat acreditats i auditable, alineats amb l'ENS.
- **ISO 20000** (Gestió de serveis TI): assegura qualitat en la gestió de serveis TI, imprescindible en un servei delegat com el MSSP.
- **ISO 9001** (Gestió de qualitat): certifica processos de qualitat general, aportant confiança en l'eficiència i millora contínua.

L'acreditació d'aquest requisit es farà mitjançant la presentació de documentació tècnica oficial del DataCenter, que haurà d'incloure:

- La seva ubicació.
- La certificació mínima TIER III, emesa per organisme de certificació acreditat.
- ISO 27001, certificació de gestió de seguretat de la informació
- ISO 20000, certificat de qualitat de serveis TI
- ISO 9001, certificació de sistemes de gestió de qualitat de servei

Aquest conjunt de certificacions garanteix seguretat, qualitat i eficiència en la prestació del servei, i són reconegudes internacionalment com a estàndards de referència.



- L'empresa licitadora haurà de presentar una relació detallada i prèvia de totes les solucions tecnològiques en modalitat SaaS (Programari com a Servei) que proposi en el marc del servei MSSP.

Aquestes solucions hauran d'estar allotjades de manera obligatòria al DataCenter especificat per a la prestació del servei, el qual haurà de complir amb els requisits establerts d'ubicació, certificació mínima TIER III i les certificacions ISO 27001, ISO 20000 i ISO 9001.

Aquest requisit garanteix que totes les solucions SaaS associades al servei es troben sota les mateixes condicions de seguretat, qualitat i disponibilitat que el DataCenter principal, assegurant la seva conformitat amb el Reial decret 311/2022 (ENS) en matèria d'integritat, disponibilitat i protecció de la informació, així com amb el Reglament (UE) 2016/679 (RGPD) i la LOPDGDD en relació amb la protecció de dades personals. D'aquesta manera es garanteix que el servei es presta amb les màximes garanties de seguretat, fiabilitat i qualitat, sense excepcions.

Mitjà d'acreditació:

- Relació documentada de totes les solucions SaaS proposades.
 - Declaració i evidència que aquestes solucions s'allotgen al DataCenter certificat indicat per a la prestació del servei MSSP.
- Quan la solució tecnològica proposada no sigui de desenvolupament propi o propietat de l'empresa licitadora, aquesta haurà d'acreditar una certificació oficial de nivell alt (p. ex. GOLD Partner) o equivalent, emesa pel fabricant de la solució.

Aquesta certificació ha de demostrar de manera inequívoca que l'empresa licitadora disposa de l'experiència i capacitat necessàries per implantar, gestionar i explotar correctament l'eina, garantint així la qualitat i seguretat del servei, assegurant que només proveïdors autoritzats i amb solvència acreditada puguin prestar el servei.

La seva acreditació serà mitjançant la presentació del certificat oficial vigent emès pel fabricant de la solució, on consti el nivell de partenariat o acreditació (mínim GOLD Partner o equivalent).

- L'empresa licitadora haurà d'acreditar que el seu equip de resposta a incidents de seguretat (CSIRT) és membre actiu, com a mínim, d'una de les següents associacions reconegudes a nivell nacional i internacional:
 - TF-CSIRT
 - CSIRT.es
 - FIRST.org

La pertinença a aquestes associacions és un requisit clau perquè:

- Garanteix la professionalitat i la fiabilitat del CSIRT, ja que aquestes organitzacions exigeixen estàndards mínims de qualitat i procediments per a l'admissió.
- Permet l'accés a informació privilegiada i actualitzada sobre amenaces, vulnerabilitats i incidents globals, que difícilment estaria disponible sense formar part d'aquestes xarxes.
- Facilita la cooperació internacional en la gestió d'incidents, millorant la capacitat de resposta davant ciberatacs transnacionals o campanyes massives.



- Aporta reconeixement i confiança institucional, ja que pertànyer a aquestes xarxes suposa ser part d'un entorn de confiança entre equips de seguretat governamentals, acadèmics i privats.
- Millora la resiliència del servei MSSP, ja que el proveïdor pot anticipar-se a noves tendències d'amenaques i aplicar mesures proactives gràcies a l'intercanvi d'informació i bones pràctiques.

La seva acreditació serà mitjançant la presentació del certificat o registre vigent que acrediti la pertinença del CSIRT a almenys una de les associacions reconegudes.

- L'adjudicatària ha d'acreditar que totes les fonts exposades en el PPT poden ser integrades al sistema de recoll·lecció de logs.

El número de fonts a integrar en el sistema de recoll·lecció de logs i correlat, quedaran determinades en els criteris del PPT i el proveïdor haurà de certificar que les pot integrar i donar el servei sota un acord de confidencialitat (NDA) i s'haurà d'acreditar mitjançant declaració responsable.

L'emmagatzemament de logs i el seu manteniment, ha de ser de mínim dos anys de retenció, ja que és imprescindible garantir que totes les fonts definides poden integrar-se de manera efectiva al sistema, assegurant així que la informació necessària per a la detecció i anàlisi de ciberincidents sigui realment disponible i exploitable; només d'aquesta manera es pot garantir la traçabilitat, la coherència de les dades i la possibilitat d'obtenir una visibilitat completa sobre els sistemes municipals.

- L'empresa haurà de presentar els certificats que acreditin les capacitats professional de les persones que participaran en el projecte.

Cal tenir en compte que degut a la durada i varietat tècnica i funcional del servei sol·licitat un mateix perfil pot ser ocupat per diverses persones al llarg del servei. Per tant, cada cop que una persona nova s'incorpori a l'equip adscrit al contracte haurà de presentar el currículum professional al responsable de contracte.

L'equip haurà d'estar integrat pel número necessari de persones per a donar el servei amb qualitat i garantia segons s'especifica al PPT relacionat amb aquesta licitació.

El contractista haurà d'assegurar al llarg de tota l'execució del contracte d'un equip mínim amb tots els perfils que s'indiquen:

Per garantir la professionalitat i solvència del servei MSSP, el personal adscrit haurà de disposar de les següents titulacions i certificacions, cadascuna d'elles amb una justificació específica:

- **Enginyeria superior en Enginyeria Informàtica o Telecomunicacions**, que aporta la base acadèmica necessària per comprendre i gestionar entorns complexos de sistemes i xarxes, assegurant una visió global i capacitat d'integració tecnològica.
- **CISA (Certified Information Systems Auditor)**, que acredita competències en auditoria de sistemes, control intern i compliment normatiu, imprescindible per verificar el grau d'adequació a l'ENS i altres marcs reguladors.
- **CISM (Certified Information Security Manager)**, que garanteix coneixements en governança i gestió estratègica de la seguretat, permetent que el servei MSSP es gestioni no només des d'un punt de vista tècnic, sinó també organitzatiu i de gestió de riscos.



- **Microsoft 365 Certified: Endpoint Administrator Associate**, que avala capacitat per administrar i protegir dispositius i aplicacions dins l'entorn Microsoft 365, assegurant el control d'una de les principals superfícies d'atac.
- **Microsoft 365 Certified: Security Administrator Associate**, que garanteix coneixements en la protecció d'identitats, accessos i informació dins de Microsoft 365, aspecte essencial per a la seguretat dels serveis cloud corporatius.
- **Microsoft Certified: Azure Security Engineer Associate**, que acredita coneixements específics en la protecció d'infraestructures i dades a Azure, assegurant la seguretat dels serveis municipals allotjats o integrats en aquest entorn.

Aquest conjunt de titulacions i certificacions assegura que el personal assignat al contracte disposa de les competències necessàries tant en l'àmbit tècnic-operatiu com en el gestor i estratègic, garantint així que el servei MSSP es presti amb les màximes garanties de qualitat, seguretat i alineament normatiu.

I. Adscripció de mitjans materials i/o personals a l'execució del contracte i Habilitació empresarial o professional i certificats acreditatius del compliment de normes o de garantia de la qualitat, de la gestió ambiental o distintius relatius a l'Esquema Nacional de Seguretat

I.1. Adscripció de mitjans personals i materials a l'execució del contracte

L'empresa licitadora haurà de complir aquests requisits de cara a l'execució del contracte i LA SEVA DISPOSICIÓ S'ACREDITARÀ PRÈVIAMENT A L'ADJUDICACIÓ, en cas de resultar adjudicatari. La manca d'acreditació suposarà la seva exclusió del procediment:

Sí ☐ No ☒

I.2. Habilitació empresarial o professional exigible per a la realització de l'activitat o servei: Sí ☐ No ☒

L'empresa licitadora haurà de complir aquests requisits de cara a l'execució del contracte i LA SEVA DISPOSICIÓ S'ACREDITARÀ PRÈVIAMENT A L'ADJUDICACIÓ, en cas de resultar adjudicatari. La manca d'acreditació suposarà la seva exclusió del procediment:

I.3. Certificats acreditatius del compliment de les normes de garantia de la qualitat i/o de gestió ambiental

L'empresa licitadora haurà de complir aquests requisits de cara a l'execució del contracte i LA SEVA DISPOSICIÓ S'ACREDITARÀ PRÈVIAMENT A L'ADJUDICACIÓ, en cas de resultar adjudicatari. La manca d'acreditació suposarà la seva exclusió del procediment:

Sí ☐ No ☒

I.4. Exigibilitat del Distintiu de Certificació de Conformitat amb l'Esquema Nacional de Seguretat o Distintiu de Declaració de Conformitat amb l'Esquema Nacional de Seguretat, del contractista i/o de la cadena de subministraments de dit contractista.

L'empresa licitadora haurà de complir aquests requisits de cara a l'execució del contracte i LA SEVA DISPOSICIÓ S'ACREDITARÀ PRÈVIAMENT A L'ADJUDICACIÓ, en cas de resultar adjudicatari. La manca d'acreditació suposarà la seva exclusió del procediment:

De conformitat amb l'informe emès pel delegat de protecció de dades de l'Ajuntament de Sant Cugat del Vallès, el cap del Servei de Tecnologia i Desenvolupament digital i el tècnic del Servei de Tecnologia i Desenvolupament digital que gestiona temes de seguretat, emès en data 22/09/2025 i que consta en l'expedient AUPAC, l'exigibilitat del distintiu de declaració certificació de conformitat amb l'Esquema Nacional de Seguretat (ENS), en relació a la contractació dels serveis objecte d'aquest contracte, és la següent:

☒ Sí, és exigible aquest distintiu per la següent categoria:

Categoria: Mitja

Justificació del distintiu exigít: Document 285995/2025

☐ No, no és exigible.

J. Criteris d'adjudicació

A) Criteris avaluable mitjançant judici de valor: fins a un màxim de 40 punts

S'estableix un llindar mínim de 20 punts en l'avaluació dels criteris de judici de valor. El no assoliment d'aquest llindar per part del licitador comportarà la seva exclusió del procediment de licitació, i per tant, no passarà a la següent fase, de conformitat amb l'article 146.3 de la LCSP i l'article 22.d) del Reial decret 817/2009.

Els criteris següents tenen per objectiu avaluar la qualitat tècnica de la proposta presentada per a la prestació del servei com a Proveïdor de Serveis Gestionats de Ciberseguretat (MSSP). Es posarà especial atenció a la coherència, maduresa, capacitat de resposta i orientació a resultats de la solució proposada, així com al seu grau d'adequació a les necessitats específiques de l'organització i al compliment del marc normatiu vigent.

A l'efecte de garantir que les ofertes presentades compleixen realment amb els requisits establerts, es valorarà específicament la defensa i la demostració pràctica (demo) de les solucions SaaS i del servei MSSP proposats. Aquesta demo permet comprovar de manera directa la viabilitat i funcionalitat de la proposta, així com el grau de compliment dels plecs, assegurant que el servei es pot prestar de forma efectiva i amb les màximes garanties de qualitat i seguretat.

La documentació presentada per a l'avaluació d'aquests criteris no podrà superar les 20 pàgines. En cas que la proposta tècnica excedeixi aquest límit, només es valorarà el contingut inclòs fins a la pàgina 20, i la resta quedarà automàticament exclosa de l'avaluació tècnica, independentment del seu contingut.

Així mateix, la proposta haurà de presentar-se en format DIN-A4, amb un cos de lletra mínim de 10 punts i interlineat senzill, utilitzant la plantilla proposada.

Per a l'avaluació de les propostes mitjançant els criteris avaluables mitjançant un judici de valor es seguirà un sistema de valoració ponderant la rellevància de les ofertes en relació als avantatges ofertats i la descripció tècnica de l'oferta.

En base a la informació continguda en aquests documents i de la comparació dels serveis oferts entre les diferents propostes dels licitadors, s'identificarà, relacionarà i avaluarà el conjunt d'avantatges previstes pels serveis objecte de valoració especificats en cada criteri de valoració. Es valorarà la rellevància del conjunt de les propostes de la següent forma (fins a dos decimals de la puntuació del subcriteri):

Rellevància nul·la o deficient:	0% de la puntuació del subcriteri.
Poc rellevants per al conjunt de la proposta:	25% de la puntuació del subcriteri.
Suficientment rellevants per al conjunt de la proposta:	50% de la puntuació del subcriteri.
Rellevants per al conjunt de la proposta:	75% de la puntuació del subcriteri.
Molt rellevants per al conjunt de la proposta:	100% de la puntuació del subcriteri

Respecte la forma de valoració, el concepte "rellevància" contemplarà en la seva valoració, la justificació detallada de la qualitat, coherència i impacte sobre els serveis, la capacitat per prestar el servei objecte del contracte, de les metodologies de treball, la optimització de recursos o mitjans destinats, la idoneïtat operativa, tecnològica, mediambiental o de qualsevol altre àmbit a valorar de les propostes previstes pels licitadors.

Per la gradació de la qualificació del concepte rellevància, es considerarà:

a) Rellevància nul·la les que derivin de l'anàlisi dels aspectes contemplats en el concepte "rellevància" i que, a criteri tècnic, suposin una descripció deficient i/o del compliment merament normatiu sobre els requeriments mínims orientatius o els exigits en el PCT i el PCAP, i/o que el seu impacte en la prestació del servei sigui considerat nul o fins i tot contraproduent sobre el conjunt del servei.

b) Propostes poc rellevants les que derivin de l'anàlisi dels aspectes contemplats en el concepte "rellevància" i que, a criteri tècnic, suposin una descripció simple o genèrica i adequada i que s'ajusta a un compliment bàsic de qualitat i/o de coherència, i que suposen un benefici limitat respecte l'assenyalat en el Plec tècnic.

c) Propostes suficientment rellevants les que derivin de l'anàlisi dels aspectes contemplats en el concepte "rellevància" i que, a criteri tècnic, suposin una descripció senzilla, poc detallada, fonamentada i argumentada que s'ajusti a un compliment suficient de qualitat i/o de coherència i/o que el seu impacte en la prestació del servei suposi un benefici lleu respecte l'assenyalat en el Plec tècnic.

d) Propostes rellevants les que derivin de l'anàlisi dels aspectes contemplats en el concepte "rellevància" i que, a criteri tècnic, suposin una descripció completa, detallada, fonamentada i argumentada que s'ajusta a un compliment notable i que continguin nivells alts de qualitat i/o de coherència i/o que el seu impacte en la prestació del servei suposi un benefici respecte l'assenyalat en el Plec tècnic.

e) Avantatges molt rellevants per al conjunt de la proposta les que derivin de l'anàlisi dels aspectes contemplats en el concepte "rellevància" i que, a criteri tècnic, suposin una descripció molt completa i detallada, ben fonamentada i argumentada, plantejades de forma específica per el contracte i que continguin nivells excel·lents de qualitat i/o de coherència i/o que el seu impacte en la prestació del servei suposi un elevat benefici respecte l'assenyalat en el Plec tècnic pel seu valor afegit o innovació.



A.1	Adequació de la solució a les necessitats del servei Es valorarà la qualitat i coherència del disseny tècnic de la solució, tenint en compte: - Es valorarà que la solució proposada s'ofereixi com a servei unificat de seguretat gestionada (MSSP), que integri de manera coordinada i centralitzada les funcionalitats de detecció, anàlisi, resposta i gestió de riscos en un únic entorn operatiu, incloent SIEM, SOC i EDR/XDR. 2 punts - L'ús d'una plataforma de seguretat unificada. 2 punts - Capacitat per a la correlació automatitzada d'esdeveniments des de múltiples fonts (sistemes, xarxa, núvol, identitats, endpoints, etc.). 2 punts - Existència d'un visor consolidat que proporcioni informació contextualitzada sobre alertes, exposició a riscos i nivells de prioritat. 2 punts - Escalabilitat de la solució i capacitat d'adaptació a l'entorn tècnic i organitzatiu del client. 2 punts - Es valorarà que la proposta inclogui un pla de millora contínua, amb propostes periòdiques de nous casos d'ús, integracions amb eines de l'organització, i automatització de processos, així com la flexibilitat per adaptar-se a canvis de l'entorn. 4 punts - Disponibilitat d'un mòdul per al compliment i seguiment de mesures de seguretat conforme al nivell mitjà o alt de l'ENS, amb funcionalitats d'auditoria contínua, gestió d'evidències, seguiment de controls i traçabilitat normativa. 4 punts Aquest criteri es fonamenta en la necessitat d'assegurar que la solució proposada s'adapta plenament a les necessitats de l'Ajuntament, garantint que la plataforma sigui unificada, escalable i capaç d'integrar-se amb l'entorn existent. Es valora que aportí funcionalitats de detecció, anàlisi i resposta avançada, així com eines de millora contínua i de compliment normatiu (ENS), ja que aquests elements són imprescindibles per garantir una gestió de la ciberseguretat eficient, sostenible i alineada amb els requisits legals i tècnics que estableix el Reial decret 311/2022 i la LCSP.	fins a	18	punts
A.2	Model de governança i seguiment del servei Es valorarà el model de supervisió i control del servei proposat, incloent: - Existència de circuits clars d'escalat, notificació i gestió d'incidents, amb temps de resposta establerts. 2 punts - Disponibilitat d'un panell de control centralitzat amb visibilitat de l'estat de la infraestructura, alertes, mètriques de servei i riscos. 3 punts	fins a	8	punts



	- Qualitat i periodicitat dels informes, així com la capacitat de personalitzar indicadors clau de rendiment (KPI) i acords de nivell de servei (SLA). 2 punts - Integració amb l'eina de ticketing pròpia de l'organització per garantir una gestió eficient i coordinada de les peticions i incidències. 1 punt És necessari valorar el model de supervisió i control del servei perquè garanteix circuits clars de gestió d'incidents, transparència en el seguiment i compliment dels SLA, assegurant que l'Ajuntament mantingui el control efectiu del servei i la seva adaptació a les necessitats reals, en coherència amb el principi de responsabilitat i control de l'ENS.			
A.3	Capacitat de detecció i resposta proactiva S'avaluarà el grau de maduresa de la solució per detectar, analitzar i respondre proactivament davant d'amenaques: - Capacitat de detecció basada en comportament, incloent tècniques d'anàlisi heurística, detecció d'activitats anòmales i puntuació de riscos. 2 punts - Integració de serveis d'intel·ligència d'amenaques contextualitzada (Threat Intelligence), que permetin adaptar els sistemes a tendències i actors específics. 2 punts - Implementació d'eines d'automatització i orquestració de resposta (SOAR – Security Orchestration, Automation and Response), per reduir el temps de resposta davant d'incidents. 2 punts - Ús d'intel·ligència artificial (IA) i aprenentatge automàtic (ML) per identificar patrons anòmals, millorar la correlació d'alertes i optimitzar la presa de decisions. 2 punts - Capacitat de la solució per generar respostes guiades o automàtiques, en funció del tipus d'amenaça, el seu impacte i la seva criticitat. 2 punts És necessari valorar la capacitat de detecció i resposta proactiva perquè la seguretat actual exigeix anticipar-se a les amenaces i reduir al mínim el temps de reacció davant incidents. Funcionalitats com la detecció basada en comportament, la intel·ligència d'amenaques, l'automatització (SOAR) i l'ús d'IA/ML asseguren una protecció més eficient i adaptada a riscos reals, garantint que l'Ajuntament disposi d'un servei capaç de prevenir, contenir i respondre ràpidament, en coherència amb l'ENS i les necessitats de continuïtat dels serveis públics.	fins a	10	punts

A.4	Defensa i demostració de la proposta S'avaluarà la demo pràctica de la solució o solucions SaaS proposades i la capacitat del licitador per defensar com es prestarà el servei MSSP, posant en evidència el compliment dels requisits i el valor que aporta a l'Ajuntament. Els aspectes a valorar són: • Qualitat i realisme de la demo de la solució (2 punts): es valorarà la claredat, usabilitat i capacitat de la demo per mostrar de manera pràctica com es compleixen els requisits funcionals i de seguretat establerts en els plecs. • Valor afegit i millores evidenciades a la demo (1 punt): es valorarà que la demo posi de manifest funcionalitats innovadores, integracions avançades o beneficis que superin els requisits mínims. • Defensa de la prestació del servei (1 punt): es valorarà la solidesa i coherència amb què el licitador explica com operarà el MSSP, com gestionarà les fonts i casos d'ús, i com garantirà el compliment normatiu i la continuïtat del servei. És necessari valorar la defensa i la demo de la proposta perquè permet comprovar de manera pràctica que les solucions SaaS presentades compleixen realment els requisits establerts, assegurant la seva viabilitat i operativitat. Aquest exercici garanteix que el licitador no només descriu sinó que demostra les funcionalitats clau, el valor afegit i les millores que ofereix la seva solució, alhora que acredita com prestarà el servei MSSP amb garanties de seguretat, qualitat i alineació amb els objectius del projecte. La presentació i defensa s'avaluaran durant una sessió presencial o virtual, prèvia acord amb l'organització, segons el que s'estipuli als plecs. Els licitadors disposaran d'un temps màxim de 20 minuts per a l'exposició, seguit d'una tanda de preguntes i respostes.	fins a	4	punts
-----	--	--------	---	-------

B) Criteris avaluable de forma automàtica: fins a un màxim de 60 punts

B.1	Preu de la part fixa Es valorarà la oferta pel preu anual del contracte que no podrà superar l'import anual del contracte identificat en el pressupost base de licitació. S'assignarà la màxima puntuació al licitador que ofereixi el preu més baix i els punts corresponents a la resta d'ofertes s'assignaran aplicant la següent fórmula: $\text{Puntuació} = \text{Màxim de punts (40)} \times ((\text{oferta més econòmica} + \text{preu licitació}) / (\text{oferta considerada} + \text{preu licitació}))$	fins a	40	punts
-----	--	--------	----	-------



	La inclusió del preu de licitació a la fórmula evita que diferències econòmiques menors entre ofertes generin variacions excessives en la puntuació final. Així, es garanteix un sistema d'avaluació just, equilibrat i transparent, on les ofertes més competitives obtenen proporcionalment una major puntuació, però sense generar distorsions significatives. Aquest mecanisme permet que la puntuació final reflecteixi de manera clara i objectiva la relació entre el preu proposat pels licitadors i la quantitat econòmica estimada pel contracte, protegint així l'interès públic i optimitzant l'ús dels recursos econòmics disponibles.			
B.2	Certificacions del personal Es valorarà que entre el conjunt del personal adscrit al servei es reuneixin les següents certificacions professionals: • Certified Red Team Professional (CRTP), 1 punts. • Certificado de Hacking Ético (CHEE), 1 punts. • Security Operations Analyst Associate (SC-200), 1 punts. • Identity and Access Administrator Associate (SC-300), 1 punts. • Cybersecurity Architect Expert (SC-100), 1 punts. Certified Red Team Professional (CRTP): acredita habilitats avançades en simulació d'atacs reals, indispensable per identificar vulnerabilitats crítiques abans que ho facin actors maliciosos. Certificado de Hacking Ético (CHEE): certifica coneixements sòlids en tècniques d'intrusió controlada, essencial per reforçar les defenses proactivament i prevenir atacs informàtics. Security Operations Analyst Associate (SC-200): acredita competències específiques en anàlisi i resposta davant incidents en entorns Microsoft, clau per assegurar una resposta ràpida i efectiva davant amenaces. Identity and Access Administrator Associate (SC-300): certifica habilitats en gestió segura d'identitats i accessos, imprescindible per prevenir violacions de seguretat relacionades amb robatori d'identitats i credencials. Cybersecurity Architect Expert (SC-100): garanteix coneixements avançats en disseny d'arquitectures segures, necessària per definir estratègies efectives i sostenibles de ciberseguretat a llarg termini. És necessari valorar les certificacions del personal perquè acreditin competències especialitzades i reconegudes internacionalment en àmbits clau de la ciberseguretat com la detecció d'amenaces, la gestió d'identitats, la resposta a incidents i el disseny d'arquitectures segures. Aquest requisit garanteix que l'equip adscrit al servei MSSP disposi de la qualificació necessària per afrontar amb solvència els reptes de seguretat i assegurar la protecció dels sistemes municipals.	fins a	5	punts
B.3	Certificacions empresa Es valorarà la certificació mínima d'empresa següent: • Esquema Nacional Seguretat (ENS) nivell ALT, 1 punt.	fins	1	punts



	Es necessari valorar la certificació d'empresa en l'ENS nivell ALT perquè ofereix un grau de seguretat superior al nivell MITJÀ, demostrant una major maduresa i solidesa en l'aplicació de mesures tècniques i organitzatives. Això garanteix més confiança en la prestació del servei MSSP i assegura que l'empresa adjudicatària està preparada per afrontar entorns crítics amb les màximes garanties de protecció.			
B.4	Compliment CCN-STIC 105 Solució proposada estigui homologada i inclosa al catàleg CCN-STIC 105, dins de la categoria Sistemes de Gestió d'Esdeveniments de Seguretat (SIEM). 1 punt Aquest criteri permet garantir que la solució de seguretat compleix amb els requisits i recomanacions del Centre Criptològic Nacional (CCN), d'acord amb el que estableix l'Esquema Nacional de Seguretat (ENS) i el Reial decret 311/2022, aportant una seguretat jurídica i tècnica addicional al servei MSSP.	fins	1	punts
B.5	Milliores recol·lecció Ampliació de fonts per la seva correlació i anàlisi. 1-5 fonts addicionals, 0,25 punts 6-10 fonts addicionals, 0,5 punts 11-15 fonts addicional, 0,75 punts 20 fonts addicionals, 1 punts Es necessari valorar la millora en la recol·lecció de fonts perquè com més fonts d'informació s'integrin, més completa i fiable serà la correlació i l'anàlisi dels esdeveniments de seguretat. L'ampliació de fonts permet obtenir una visibilitat més gran de l'entorn tecnològic municipal, reduir punts cecs i millorar la detecció proactiva d'amenaques, tot això sense cost addicional per a l'Ajuntament.	fins	1	punts
B.6	Preu de la part variable Oferta econòmica de preus unitaris: S'assignarà la màxima puntuació al licitador que ofereixi el preu més baix en cadascun dels preus unitaris i els punts corresponents a la resta d'ofertes s'assignaran aplicant la següent fórmula: $\text{Puntuació} = \text{Màxim de punts} \times (\text{oferta més econòmica} / \text{oferta considerada})$ - Preu/hora Tècnic N1, 0,5 punts - Preu/hora Tècnic N2, 0,5 punts - Preu/hora CSIRT, 0,5 punts - Preu/hora DFIR, 0,5 punts	fins a	2	punts
B.7	Milliores servei Pla de formació en ciberseguretat per a usuaris finals	fins a	10	punts

	És una millora clau dins del servei MSSP, ja que redueix el risc derivat de l'error humà, millora la cultura de seguretat a l'organització i reforça el compliment normatiu. A més, forma el personal com a part activa de la protecció, augmentant la resiliència davant amenaces digitals. Aquestes formacions han de contemplar aquests aspectes: Formació presencial: Sessions formatives amb una periodicitat trimestral, realitzades en grups de fins a 40 persones, per garantir una interacció directa i l'adaptació dels continguts al perfil dels assistents. Formació telemàtica: Sessions formatives també trimestrals, impartides en format webinar o a través de plataformes tipus Moodle o equivalents, amb material didàctic complet posat a disposició de tota la plantilla, assegurant-ne l'accessibilitat, la traçabilitat i l'avaluació contínua. Píndoles formatives: Enviament mensual d'una píndola formativa en CiberSeguretat, amb continguts breus, pràctics i adaptats a situacions reals, per mantenir una sensibilització constant sobre bones pràctiques i nous riscos. • Formació presencial, 2 punts • Formació telemàtica, 2 punts • Píndoles formatives, 2 punts Formació presencial: Permet treballar la conscienciació en grups reduïts amb interacció directa, adaptant els continguts a l'organització. És clau per reforçar la responsabilitat individual i col·lectiva en la seguretat digital. Formació telemàtica: Garanteix l'accessibilitat de la formació a tota la plantilla, amb traçabilitat i seguiment. Complementa la protecció tècnica del MSSP amb coneixement pràctic i continu, disponible en qualsevol moment. Píndoles formatives: Ofereixen recordatoris mensuals breus i útils per mantenir l'atenció en bones pràctiques digitals. Són una eina àgil i eficaç per mantenir la sensibilització activa de forma sostinguda. Totes les activitats formatives tant presencials com telemàtiques, incloses les píndoles mensuals es duren a terme íntegrament en llengua catalana. A més, les temàtiques i continguts concrets de totes les formacions seran pactats prèviament amb l'organització, tenint en compte les necessitats específiques dels diferents perfils professionals i els riscos més rellevants per al seu entorn tecnològic. Incorporació del servei de vigilància digital Com a millora dins dels serveis gestionats de seguretat (MSSP), es proposa la incorporació d'un servei específic de vigilància digital, amb l'objectiu d'ampliar la capacitat de detecció proactiva més enllà del perímetre clàssic de la infraestructura tecnològica. • Monitoratge d'exposició de dades, 1 punt • Protecció de la reputació digital, 1 punt			
--	--	--	--	--



• Intel·ligència d'amenaques (Threat Intelligence), 1 punts • Monitoratge del compliment i riscos normatius, 1 punts Monitoratge d'exposició de dades: Permet detectar fuites de credencials o informació sensible en entorns públics o il·lícits, anticipant possibles incidents i activant mesures preventives. Protecció de la reputació digital: Identifica usos fraudulents de la marca, dominis enganyosos o continguts difamatoris, evitant danys d'imatge i suplantacions. Intel·ligència d'amenaques: Aporta informació actualitzada sobre riscos externs i actors amenaçadors, millorant la capacitat de detecció i resposta. Monitoratge del compliment normatiu: Ajuda a identificar exposicions de dades o pràctiques de risc que podrien suposar incompliments legals, evitant sancions i garantint el compliment de normatives com RGPD o ENS.			
--	--	--	--

K. Criteris per a la determinació de l'existència de baixes presumptament anormals

☒ Opció 3: Diversos criteris d'adjudicació

Vist que es regulen diversos criteris d'adjudicació, de conformitat amb l'article 149 de la LCSP, per a la determinació de si les ofertes presenten valors anormals o desproporcionats s'ha de dur a terme en funció dels límits i els paràmetres objectius establerts a continuació que :

· Si concorre una empresa licitadora, es considera que l'oferta és anormal si compleix els dos criteris següents:

- Que l'oferta econòmica sigui un 25% més baixa que el pressupost de licitació.
- Que la puntuació que li correspongui en la resta de criteris d'adjudicació diferents del preu sigui superior al 80% de la puntuació total.

· Si concorren dues empreses licitadores, es considera oferta anormal la que compleixi el criteri següent:

- Que la puntuació total que li correspongui en la suma de punts de tots els criteris d'adjudicació sigui superior en més d'un 20% a la puntuació total més baixa.

· Si concorren tres o més empreses licitadores, es considera oferta anormal la que compleixi un dels dos criteris següents:

- Quan no hi hagi cap puntuació per sota del 90% de la mitjana aritmètica de totes les puntuacions: que la puntuació de la oferta sigui superior en més d'un 10% a la mitjana aritmètica de totes les puntuacions.
- Quan hi hagi puntuacions per sota del 90% de la mitjana aritmètica de totes les puntuacions: que, un cop excloses les puntuacions inferiors al 90% de la mitjana aritmètica de totes les puntuacions, la puntuació de la oferta sigui superior en més d'un 10% a la mitjana aritmètica de les puntuacions que no han estat excloses.

Justificació fórmula escollida: La licitació incorpora múltiples criteris, tant tècnics com econòmics, que poden generar desequilibris entre qualitat i preu. Per això, s'estableixen

paràmetres objectius que permetin detectar ofertes anormalment baixes i garantir-ne la viabilitat.

L. Condicions especials d'execució i obligacions de caràcter essencial

- Condicions especials d'execució de tipus social o medi ambiental

L'empresa mantindrà, durant la vigència del contracte, les condicions laborals i socials de les persones treballadores ocupades en l'execució del contracte, fixades en el moment de presentar l'oferta, segons el conveni que sigui d'aplicació. L'incompliment podrà ser objecte de penalització com a falta molt greu o causa d'extinció contractual.

Justificació condició exigida: D'acord l'article 202 de la LCSP s'exigeix una condició especial de tipus social.

- Condicions i/o obligacions que tenen la consideració d'obligació essencial

Es considera procedent aplicar una condició de tipus de transparència fiscal, la qual consistirà:

El contractista es compromet a executar el contracte amb criteris de transparència fiscal, per la qual cosa els ingressos o beneficis procedents d'aquest contracte públic han de ser íntegrament declarats i tributats d'acord amb la legislació fiscal vigent.

L'empresa adjudicatària ha de presentar una declaració responsable comproment-se, que en l'execució del contracte s'han complert les obligacions derivades de les disposicions vigents d'acord amb la legislació fiscal.

M. Cessió del contracte

- ☒ Sí, en els termes de l'article 214 de la LCSP
☐ No

N. Subcontractació

Es permet la subcontractació de conformitat amb l'art. 215 de la LCSP.

O. Tramitació i pagament de les factures:

O.1 Periodicitat del pagament:

- ☐ Anual
☒ Mensual
☐ Trimestral
☐ Altres:

O.2 Forma de pagament:

- ☒ Per la part variable: d'acord amb els **preus unitaris** oferts, pels serveis efectivament executats
☒ Per la part fixa: d'acord amb la **part proporcional del preu total ofert**, segons la periodicitat del pagament
☐ Altres:

O.3. La documentació a presentar junt amb la factura és la següent:



x

Albarans o fulls de treball que acreditin el lliurament de les prestacions facturades.

Documents que acreditin el compliment d'altres obligacions contractuals:

--

P. Revisió de preus

Sí ☐ No ☒

Fórmula aplicable (*en el seu cas*):

Justificació: De conformitat amb les previsions de l'article 103 de la LCSP

Q. Termini de garantia

Sí ☒

Aquest termini començarà a computar a partir de la data de recepció o conformitat del servei, i aquest serà de 6 mesos, d'acord amb el que estableix l'article 210.3 de la LCSP.

No ☐ atès que

R. Programa de treball

Sí ☒ No ☐

S. Penalitats

Les penalitzacions previstes per aquesta licitació són les següents:

- Donat que l'objecte del contracte és la substitució del servei CUGAT-SOC actual, l'adjudicatari haurà de garantir la posada en marxa operativa i efectiva del nou servei en un termini màxim de dos mesos a comptar des de la data d'acta d'inici de servei d'acord amb el calendari següent:
 - Primer mes (a comptar des de l'acta d'inici del servei): hauran d'estar implantats i operatius com a mínim el 50% de les fonts i casos d'ús (CdU), prioritzant els sistemes més crítics.
 - Segon mes: el servei haurà d'estar completament operatiu, amb el 100% de les fonts i CdU integrats i validades.

En cas de no complir aquest termini, l'empresa adjudicatària:

- **No podrà emetre cap factura ni percebre cap import** derivat del nou contracte fins que el servei sigui plenament operatiu.

Aquesta condició actuarà com a condició suspensiva per a qualsevol obligació de pagament a càrrec de l'Ajuntament, de manera que no es podrà emetre cap factura ni percebre cap import fins que el servei sigui plenament operatiu.

Increment temps fase	Penalització
No assolir el 50% de la fase 0 del PPT al primer mes	10% de l'import anual acumulable del contracte per cada setmana de retard amb un màxim del 50%.
No assolir el 100% de la fase 0 del PPT al segon mes	10% de l'import anual acumulable del contracte per cada setmana de retard amb un màxim del 50%.
Retard superior a 10 setmanes des de l'acta d'inici	Resolució del contracte i execució de garanties.

- Per l'increment en el temps de resposta en incidents relacionats amb manteniment, revisió, administració i reporting de la infraestructura de seguretat (definit al PPT), es penalitzarà, per motius directament imputables a l'adjudicatari segons el quadre establert.

Increment temps de resposta	Penalització
Increment del temps en 1 hora en nivell CRITIC (60 minuts)	1% de l'import del contracte
Increment del temps en 2 hores en nivell CRITIC (120 minuts)	2% de l'import del contracte
Increment del temps en 3 hores en nivell CRITIC (180 minuts)	5% de l'import del contracte
Increment del temps en 2 hores en nivell ALT (120 minuts)	1% de l'import del contracte
Increment del temps en 3 hores en nivell ALT (180 minuts)	2% de l'import del contracte

- Per l'increment en el temps de resolució en incidents relacionats amb manteniment, revisió, administració i reporting de la infraestructura de seguretat (definit al PPT), es penalitzarà, per motius directament imputables a l'adjudicatari segons el quadre establert.

Increment temps de resolució	Penalització
Increment del temps en 1 hora en nivell CRITIC (60 minuts)	1% de l'import del contracte
Increment del temps en 2 hores en nivell CRITIC (120 minuts)	2% de l'import del contracte
Increment del temps en 3 hores en nivell CRITIC (180 minuts)	5% de l'import del contracte
Increment del temps en 2 hores en nivell ALT (120 minuts)	1% de l'import del contracte
Increment del temps en 3 hores en nivell ALT (180 minuts)	2% de l'import del contracte

- Per l'increment en el temps de resposta i inici i realitzacions de tasques en incidents relacionats amb la gestió i la resposta a incidents de seguretat (definit al PPT), es penalitzarà, per motius directament imputables a l'adjudicatari segons el quadre establert.

Increment temps de accions	Penalització
Increment del temps en 1 hora en nivell CRITIC (60 minuts)	2% de l'import del contracte
Increment del temps en 2 hores en nivell CRITIC (120 minuts)	3% de l'import del contracte
Increment del temps en 3 hores en nivell CRITIC (180 minuts)	5% de l'import del contracte
Increment del temps en 2 hores en nivell ALT (120 minuts)	1% de l'import del contracte
Increment del temps en 3 hores en nivell ALT (180 minuts)	2% de l'import del contracte

a) Infraccions molt greus:

- L'incompliment o compliment defectuós, per part del contractista o subcontractista, de les obligacions i/o condicions d'execució del contracte establertes en els plecs de condicions i/o en l'oferta, quan produeixi un perjudici molt greu i no doni lloc a la resolució del contracte.
- L'incompliment de les obligacions en matèria mediambiental, socials o laborals establertes pel dret de La Unió Europea, el dret nacional, els convenis col·lectius o per les disposicions de dret internacional mediambiental, social i laboral que vinculen l'Estat i en particular dels establerts a l'annex V de la Llei 9/2017, de 8 de novembre, de contractes del sector públic.
- Impedir o dificultar les tasques de supervisió i control del servei per part del responsable del contracte, o bé realitzar accions que posin en risc l'interès públic.
- L'incompliment de la confidencialitat de les dades.
- L'incompliment de qualsevol dels aspectes i compromisos presentats a l'oferta i valorats mitjançant algun criteri d'adjudicació.
- Realitzar conductes que tinguin per objecte o puguin produir l'efecte d'impedir, restringir o falsejar la competència com per exemple els comportaments col·lusoris o de competència fraudulenta (ofertes de resguard, eliminació d'ofertes, assignació de mercats, rotació d'ofertes, etc.).
- L'incompliment de les clàusules que són essencials en el contracte, incloent-hi les condicions especials d'execució establertes d'acord amb l'assenyalat en l'article 202.
- L'incompliment de l'adscripció de mitjans personals o materials suficients per a la correcta execució del contracte.
- L'incompliment de les condicions i prescripcions ofertes i valorades mitjançant els criteris d'adjudicació.
- Reincidència en la comissió de tres faltes greus
- Totes aquelles que s'hagin qualificat com a tal en els plecs tècnics.

b) Infraccions greus:

- L'incompliment o compliment defectuós, per part del contractista o subcontractista, de les obligacions i/o condicions d'execució del contracte establertes en els plecs de condicions o en l'oferta, quan constitueixi un perjudici greu.



- Desobediència en les indicacions efectuades pel responsable del contracte en relació a la prestació
- No posar en coneixement del responsable del contracte prèviament a la celebració de qualsevol acte de publicitat o difusió de l'empresa adjudicatària relativa a l'objecte d'aquest contracte.
- No observar els principis, les normes i els cànons ètics propis de les activitats, els oficis i/o les professions corresponents a les prestacions objecte dels contractes.
- No col·laborar amb l'òrgan de contractació en les actuacions que aquest realitzi per al seguiment i/o l'avaluació del compliment del contracte, particularment facilitant la informació que li sigui sol·licitada per a aquestes finalitats i que la legislació de transparència i els contractes del sector públic imposen als adjudicataris en relació amb l'Administració o administracions de referència, sens perjudici del compliment de les obligacions de transparència que els pertoquin de forma directa per previsió legal.
- Reincidència en la comissió de tres faltes lleus.
- No complir amb els terminis parcials d'entrega dels treballs o la realització dels serveis establerts al plec de condicions tècniques o en la pròpia oferta.
- En cas d'incompliment de l'obligació d'informació sobre les condicions de subrogació en contractes de treball que determina l'article 130 de la LCSP.
- Totes aquelles que s'hagin qualificat com a tal en aquest plecs tècnics.

c) Infraccions lleus:

- L'incompliment o compliment defectuós, per part del contractista o subcontractista, de les obligacions i/o condicions d'execució del contracte establertes en els plecs de condicions o en l'oferta, quan no constitueixi falta molt greu o greu.
- No comunicar immediatament al responsable del contracte les deficiències o irregularitats en la prestació del servei.
- L'incompliment de les obligacions de caràcter formal o documental exigides en la normativa de prevenció de riscos laborals i que no estiguin tipificades com a greus o molt greus.
- Aquells incompliments no previstos anteriorment i que suposin l'incompliment de les obligacions o condicions establertes en aquest plec o el plec de prescripcions tècniques.
- Independentment del rescabament per danys i perjudicis, en cas d'incompliment que no produeixi resolució del contracte es podran aplicar les penalitzacions següents:
 - o Faltes molt greus: multa de fins a un 10% del preu del contracte, entès com al pressupost del contracte.
 - o Faltes greus: multa de fins a un 6 % del preu del contracte, entès com al pressupost del contracte.
 - o Faltes lleus: multa de fins a un 3 % del preu del contracte, entès com al pressupost del contracte.

En el cas de no assistir a les reunions de coordinació i seguiment que puguin organitzar-se durant l'execució s'aplicarà una penalització d'un 0,5% del preu total de licitació del conjunt de contracte.

Les penalitzacions previstes en aquest apartat (S. Penalitats) es consideren justificades, asseguruen la correcta execució del contracte, suposen un mecanisme per responsabilitzar al adjudicatari de les desviacions indegudes i dels incompliments de les seves obligacions.

T. Assegurances

T1. Tipus: Assegurança de responsabilitat civil per riscos professionals que haurà d'estar en vigor durant tot el termini de vigència del contracte i el termini de garantia.



T2. Suma mínima assegurada: 1.000.000 € i per víctima de 600.000 €

U. Responsable del contracte i unitat encarregada del seguiment i l'execució ordinària del contracte

Responsable del contracte: Alberto Martinez, Responsable de Seguretat de l'Ajuntament de Sant Cugat del Vallès

V. Garanties

Garantia definitiva

· S'exigeix la constitució de garantia definitiva?

☐ No, en aquest contracte s'eximeix la constitució de garantia pels motius que es detallen a continuació:

☒ Sí, i aquesta es constituirà en els termes següents:

☐ 5% del preu final ofert pel licitador (IVA exclòs).

☐ 5% del preu base de licitació (IVA exclòs).

☒ 5% de preu final ofert pel licitador (IVA exclòs) de la part fixa + 5% del pressupost base de licitació (IVA exclòs) de la part variable.

· Es preveu la necessitat de constituir una garantia definitiva complementària de conformitat amb les previsions de l'article 107.2 de la LCSP?

Sí ☐ No ☒

- en tots els supòsits ☐

- només en el supòsit que l'oferta de l'adjudicatari hagués estat inicialment incursa en presumpció d'anormalitat ☒

Percentatge de la garantia complementària: 5 % del preu final ofert pel licitador (IVA exclos), és a dir la garantia definitiva total a constituir serà d'un 10 % del preu final ofert pel licitador (IVA exclòs).

W. Existència de personal susceptible de subrogació d'acord amb el que regula l'article 130 LCSP:

L'actual contractista ha declarat l'existència de personal susceptible de subrogació d'acord amb el que regula l'article 130 de la LCSP:

Sí ☐, segons el conveni col·lectiu que és el conveni de referència aplicat per l'empresa contractista actual.

No ☒

X. Cessió de dades al contractista

☐ No

☒ Sí

Denominació de l'activitat de tractament:

Responsable del tractament de les dades personals: (òrgan de contractació i correu electrònic de contacte)

Finalitat: (finalitat o finalitats per a les quals es fa el tractament)

En cas que hi hagi cessió de dades al contractista, el contractista haurà de signar el contracte, d'encarregat del tractament, que s'incorpora com a **annex 4 d'aquest PCAP**.

De conformitat amb la legislació, europea i espanyola, de protecció de dades de caràcter personal, els titulars de les dades personals podran exercitar els drets d'accés, rectificació, supressió, limitació, portabilitat i, si escau, oposició, mitjançant la remissió d'un escrit dirigit a Ajuntament de Sant Cugat del Vallès, Atenció Ciutadana, Plaça de la Vila, 1, 08172 Sant Cugat del Vallès, indicant "Ref. Protecció de dades" o bé exercir el seu dret a través de la Seu Electrònica, mitjançant el tràmit N149 Gestió dels drets de dades personals.

Per a més informació es pot consultar la pàgina web: <https://www.santcugat.cat/web/proteccio-de-dades>. En cas d'estimar una vulneració del dret a la protecció de dades, podrà presentar una reclamació, en primer lloc, davant el nostre Delegat de Protecció de Dades dpd@santcugat.cat o, si escau, davant l'Autoritat Catalana de Protecció de Dades <https://apdcat.gencat.cat/ca/inici/>

Y. Constitució de la Mesa de Contractació:

☐ No, d'acord amb el que preveu l'article 326.1 de la LCSP serà potestativa la constitució de la Mesa de contractació en el procediment obert simplificat abreujat recollit a l'article 159.6 de la LCSP.

☒ Sí, la Mesa de contractació estarà integrada pels membres que es determinen en l'acord del Ple d'aprovació de la composició i les normes de funcionament de la Mesa Permanent de Contractació de l'Ajuntament de Sant Cugat del Vallès.

(https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/cap.pscp?reqCode=viewDetail&idCap=3045974)

Concretament, respecte el vocal tècnic de la Mesa, aquest serà:

TITULAR (la persona nomenada com a responsable del contracte)

Nom i cognoms: Alberto Martinez

Càrrec: Responsable de Seguretat

Proposta de vocals tècnics de la Mesa de Contractació

Nom i cognoms: Sergi Jerez Rico.

Càrrec: Director de Tecnologia

Nom i cognoms: Alex Clotet Fort.

Càrrec: Cap de la Secció de Sistemes.

Z. Tinència d'Alcaldia de l'àmbit del Servei promotor del contracte

Denominació de la Tinència: Relacions Institucionals, Bon Govern i Ciutat Digital.

Nom i cognoms del Tinent/a: Jordi Puigneró i Ferrer

ANNEX 1 . Informe tècnic de justificació del pressupost de licitació

De conformitat amb els articles 100, 101 i l'article 116.4, lletra d) de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic (en endavant, LCSP), el present informe s'emet als efectes de justificar el pressupost de licitació

El present concurs està basat en serveis tecnològics que es requereixen per al manteniment dels sistemes d'informació existents i el desenvolupament dels plans estratègics. Les partides corresponents als serveis tecnològics, estan basades en preus/hora de mà d'obra, en funció de la categoria dels treballadors que participin en els treballs.

Per poder avaluar aquets pressupost, s'ha fet servir, la taula de tarifes del sector de la enginyeria de sistemes, publicades en el Boletín Oficial del Estado (BOE) amb data del dimarts 16 d'octubre del 2018 i l'actualització BOE-A-2023-25866, titulats corresponentment:

“Resolución 330/38255/2018, de 28 de septiembre, de la Dirección General de Asuntos Económicos, por la que se aprueban las tarifas de Ingeniería de Sistemas para la Defensa de España SA, S.M.E., M.P.”

“Resolución 330/38477/2023, de 30 de noviembre, de la Dirección General de Asuntos Económicos, por la que se aprueban las tarifas de Ingeniería de Sistemas para la Defensa de España, SA, S.M.E., M.P.”

A l'apartat 1.1 de l'anomenat document amb referencia BOE-A-2018-14164 trobem la taula de tarifes/hora en la que ens basat per poder fer el pressupost:

1.1 Tarifas Hora para las actividades de Consultoría y Asistencia Técnica en Áreas Tecnológicas de Seguridad, Defensa, Administración Pública, Transporte y Tecnologías de la información y las Comunicaciones.

Actividad	Categoría	Tarifa hora anterior - (C/Hora)	Tarifa hora - (C/hora)
Consultoría.	Gerente.	88,12	96,85
	Jefe Proyecto.	76,46	84,04
	Consultor Principal.	65,68	72,19
	Consultor Senior.	54,44	59,84
	Consultor Junior.	45,21	49,69
Asistencia técnica.	Coordinador.	68,66	75,46
	Técnico Experto A.	64,97	71,41
	Técnico Experto B.	54,24	59,62
	Técnico Experto C.	46,61	51,23
	Administrativo.	44,3	48,69

A l'apartat 1 de l'anomenat document amb referència BOE-A-2023-25866 trobem la taula actualitzada de algunes categories de tarifes/hora en la que ens basat per poder fer el pressupost:

1. Tarifas.

Aprobar las Tarifas de la Sociedad Mercantil Estatal Ingeniería de Sistemas para la Defensa de España SA, SME, MP (ISDEFE), aplicables a efectos de lo dispuesto en el artículo 32 de la Ley de Contratos del Sector Público. Las tarifas que se aprueban son las siguientes:

Agrupación categorías	Tarifa 2024 (Euros/hora)	Tarifa semanal Euros
Jefe/Coordinador.	79,47	2.980,30
Consultor A.	75,44	2.829,01
Consultor B.	64,32	2.411,97
Consultor C.	56,70	2.126,17
Consultor D.	48,44	1.816,32
Técnico.	42,40	1.589,96
Administrativo.	47,34	1.775,40

Aquestes tarifes ja inclouen un marge del 4% i un 2% de desviacions i imprevistos, així com un 2% de disponibilitat del personal i com especifica el document, a l'aparat 1.3, aquestes tarifes inclouen els costos directes i indirectes assignables a les hores de treball de les diferents categories de la taula, així com les despeses generals i el marge per a imprevistos i desviacions.

A) Part fixa del contracte

El pressupost del present contracte esta format per una part fixe i una part variable. Els preus corresponents al servei tecnològics estan referenciats al quadre de preu/tarifa adjunts al present document.

En les següents taules es pot veure la previsió d'hores de les diferents categories del personal, aquestes taules varien en el transcurs de l'execució del contracte perquè es preveu una diferent dedicació durant l'execució del contracte.

SERVEIS	Categoria	Hores/any	€/hora	Dedicació	Import
Security Manager	Cap de projecte	1095	80,00 €	10%	8.760,00 €
Tècnic CSIRT	Tècnic expert A	1460	71,00 €	8%	8.292,80 €
RedTeam	Tècnic expert A	56	71,00 €	100%	3.976,00 €
Tècnic N2	Tècnic expert B	4380	60,00 €	8%	21.024,00 €
Tècnic N1	Tècnic expert C	8760	51,00 €	8%	35.740,80 €
Plataforma de Seguridad	Llicències				60.000,00 €
SIEM	Llicències				20.000,00 €

B) Part variable del contracte

Serveis addicionals en assessorament tècnic i jurídic. La part variable està formada per els conceptes que indica la següent taula i es pagarà mensualment segons l'execució.

En les següents taules es pot veure la previsió d'hores de les diferents categories del personal, aquestes taules varien en el transcurs de l'execució del contracte perquè es preveu una diferent dedicació durant l'execució del contracte.

SERVEIS	Categoria	Hores/any	€/hora	Import
Jornada Tècnic N2	Tècnic expert B	60	60,00 €	3.600,00 €
Jornada Tècnic N1	Tècnic expert C	60	51,00 €	3.060,00 €
Jornada DFIR	Tècnic expert A	70	71,00 €	4.970,00 €
Jornada CSIRT	Tècnic expert A	40	71,00 €	2.840,00 €

C) Pressupost anual màxim estimatiu

El resum del pressupost anual del contracte en funció del detall anterior és el següent:

Total (Part Fitxa + Variable)	Any 1	Any 2	Any 3	Any 4	Import total
Preu base de licitació	172.263,60 €	172.263,60 €	172.263,60 €	172.263,60 €	689.054,40 €
IVA (21%)	36.175,36 €	36.175,36 €	36.175,36 €	36.175,36 €	144.701,42 €
Total	208.438,96 €	208.438,96 €	208.438,96 €	208.438,96 €	833.755,82 €

ANNEX 3 . Informe d'accés a recursos tecnològics i adquisició, desenvolupament i/o manteniment d'aplicacions i pàgines webs.

A. La contractació requereix accés a recursos tecnològics?

- ☒ Sí
☐ No (*)

(*) El Servei de Tecnologia i Desenvolupament Digital no podrà garantir la disponibilitat de recursos si aquests no s'han tingut en compte prèviament

A.1. Projecte o ús que es donarà al servidor:

Es necessari muntar internament un servidor amb la funció de collector de logs

A.2. Connectivitat i Telecomunicacions

Necessitats de connectivitat des d'Internet:

Es necessari sortida a internet

A.3. Infraestructures de Processament de Dades

Fins no tenir adjudicatari no es possible tenir aquestes dades.

A.4. Equipaments informàtics al lloc de treball: NO

() D'acord amb la IT-GQ-37 [DISPOSICIÓ DE RECURSOS D'INFRAESTRUCTURA DEL LLOC DE TREBALL], l'ajuntament proporcionarà, únicament, els punts d'accés a xarxa no corporativa [Internet]. Si la contractació de serveis implica la gestió de persones, l'empresa adjudicatària haurà de proporcionar i serà responsable de l'equipament informàtic i de telefonia amb el programari necessari per oferir el servei.*

A.5. Quantitat i modalitat d'equipaments informàtics als llocs de treball a proveir

Client lleuger:

Ordinador personal:

Estació de treball gràfica:

Altres:

() L'ajuntament únicament proporcionarà aquells llocs de treball en els que sigui necessari utilitzar un programari corporatiu específic per al desenvolupament del servei contractat [p.ex. punt de venda d'entrades del museu]*

A.6. Equipaments de xarxa:

A.7. Equipaments de telefonia:

(*) L'ajuntament únicament proporcionarà aquells llocs de treball en els que sigui necessari utilitzar un programari corporatiu específic per al desenvolupament del servei contractat [p.ex. punt de venda d'entrades del museu]

A.8. Observacions:

B. La contractació requereix l'adquisició, desenvolupament i manteniment d'aplicacions per a dispositius mòbils, programes d'ordinador o pàgines web?

- ☐ Sí
☒ No

En cas afirmatiu, omplir:

B.1. La contractació té per objecte l'adquisició, desenvolupament i manteniment d'una aplicació?

- ☐ Sí
☒ No

En cas afirmatiu, d'acord amb l'article 157 de la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic, s'ha d'efectuar les pertinents consultes al directori general d'aplicacions https://administracionelectronica.gob.es/ctt/CTTprincipalEs.htm?urlMagnolia=/pae_Home/pae_SolucionesCTT.html#.YguhBUNKiUk) i acreditar que:

☐ No existeix cap solució disponible que pugui satisfer total o parcialment les necessitats que motiven el contracte proposat.

☐ Existeix una solució disponible que pot satisfer total o parcialment les necessitats que motiven el contracte proposat, però no es considera adient en termes d'eficiència pels motius següents:

B.2. L'aplicació requereix d'una gestió d'usuaris:

- ☐ Sí
☒ No

Es requereix la integració amb el sistema de gestió d'usuaris de l'Ajuntament?

- ☐ Sí
☒ No

(*)Totes les aplicacions que tinguin gestió d'usuaris s'han d'integrar al sistema de gestió d'usuaris de l'Ajuntament [directori actiu].

B.1. La contractació contempla mesures d'accessibilitat, d'acord amb allò establert el Reial Decret 1112/2018?

- ☐ Sí
☒ No

En cas afirmatiu, quines mesures s'han adoptat per garantir que es donarà compliment a l'establert al Reial Decret 1112/2018, de 7 de setembre sobre accessibilitat dels llocs web i aplicacions per a dispositius mòbils o programari d'ordinador (i per tant la norma UNE-EN 301549:2022 de requisits d'accessibilitat per productes i serveis TIC), durant la totalitat de la vigència del contracte?

B.3. Mesures previstes per facilitar el retorn del producte i l'eventual contractació amb tercers, un cop finalitzi el termini d'execució del contracte:

No

B.4. Avaluació de possibles costos no inclosos a la contractació que poden repercutir-se a l'Ajuntament (costos de manteniment no inclosos a la contractació, etc.)

No

B.5. El servei té pressupost consignat, a efectes de dur a terme l'auditoria obligatòria d'accessibilitat, de l'aplicació per a mòbil o de la pàgina web?

- ☐ Sí
☒ No

Quantitat:

No aplica

Consideracions finals

Un cop adjudicat el contracte es requerirà al responsable municipal del contracte l'entrega de la següent documentació, segons quin hagi estat l'objecte del contracte, per tal de garantir el bon funcionament, explotació i manteniment dins l'arquitectura de sistemes de l'ajuntament :

- Esquema de la solució final adoptada
- Manual d'administració de l'Aplicació
- Manual d'administració de Sistemes
- Manual d'arquitectura de Sistemes

() És convenient preveure al PPT que l'empresa contractista entregui aquesta documentació al responsable del contracte abans de l'inici de la prestació contractual.*

