

MEMÒRIA JUSTIFICATIVA DE CONFORMITAT AMB L'ARTICLE 116 DE LA LCSP SOBRE EL CONTRACTE BASAT EN L'ACORD MARC DE SERVEIS DE SUPPORT A LES FUNCIONS DE CIBERSEGURETAT PRÒPIES DEL CENTRE D'OPERACIONS DE SEGURETAT DE L'AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA AMB NÚMERO D'EXPEDIENT AM.02.2024 PER A LA CONTRACTACIÓ D'UN SERVEI DE SUPORT PEL DESENVOLUPAMENT D'UN ANALISTA VIRTUAL (LOT 2)

L'Objecte de la present memòria és la justificació de les necessitats de l'Agència de Ciberseguretat de Catalunya per a la formalització d'un contracte de serveis de suport pel desenvolupament d'un analista virtual que permeti millorar l'eficiència operativa de l'Àrea d'operació de la seguretat garantint un impacte positiu en la ciutadania al millorar el temps de detecció i resposta en els ciberatacs i per tant reduint la finestra d'exposició.

El present contracte està finançat per la unió europea, mitjançant els fons del Pla de Recuperació, Transformació i Resiliència.

OBJECTE DEL CONTRACTE

Objecte: Contractació d'un servei de suport pel desenvolupament d'un analista virtual que permeti millorar l'eficiència operativa de l'Àrea d'operació de la seguretat garantint un impacte positiu en la ciutadania al millorar el temps de detecció i resposta en els ciberatacs i per tant reduint la finestra d'exposició.

Tipus: Contracte de serveis-

Expedient: CB25AMOP2B002

Procediment: Procediment basat de l'acord marc amb número d'expedient AM.02.2024

CPV: 72510000- Serveis de Gestió relacionats amb la informàtica

Finançament afectat: si. Data d'aprovació del conveni i les entitats. Import total concedit 15.000.000 aportació de INCIBE (75%).

Data conveni: 18 de Desembre de 2023

JUSTIFICACIÓ DE LA CONTRACTACIÓ I NECESSITATS

El present contracte podrà estar finançat fins a un 100% per la Unió Europea NextGenerationUE.

La contractació objecte del present informe resulta necessària per a la realització del compliment i les finalitats institucionals de l'Agència de Ciberseguretat de Catalunya, especialment per a l'acompliment dels objectius.

L'agència de Ciberseguretat de Catalunya té la consideració d'Administració Pública a efectes de la Llei 9/2017 de Contractes del Sector Públic "LCSP". Sens perjudici d'això,

a altres efectes, aquesta entitat resta subjecta al Decret legislatiu 2/2002, de 24 de desembre, pel qual s'aprova el Text refós de la Llei 4/1985, de 29 de març, de l'Estatut de l'Empresa Pública Catalana, sent en conseqüència, una entitat de Dret públic, en general subjecta en la seva activitat al Dret privat.

En un context altament canviant i exigent, en la incorporació de noves capacitats/serveis/recursos/coneixements, com és el món de la ciberseguretat, i més concretament, el món de la ciberseguretat en el context públic, l'Agència de Ciberseguretat es troba immersa un gran creixement per la qual les licitacions augmenten de manera directament proporcional al creixement de la entitat pública.

Els darrers anys han estat marcats per la pandèmia de la COVID-19, impactant la mateixa fortament en diverses àrees tant del sector privat com del sector públic. Amb motiu de la mateixa es van succeir diversos danys socials i impactes econòmics a aquests sectors que necessiten ésser reparats i recuperats. Aquesta situació va justificar l'aprovació d'un paquet de mesures d'ajut de gran abast pel Consell Europeu en data 21 de juliol de 2020.

Entre aquestes mesures, dins del Pla per la recuperació per Europa, el Consell Europeu va posar en marxa un Instrument Europeu de Recuperació (el programa Next Generation EU) per estimular la recuperació econòmica i la reparació dels danys causats per la pandèmia.

El programa contempla dos instruments financers: (i) El Mecanisme Europeu de Recuperació i Resiliència (en endavant, MRR) i (ii) L'ajuda a la Recuperació per a la Cohesió i els Territoris d'Europa (REACT-UE).

En data 12 de febrer de 2021 es va aprovar el Reglament (UE) 2021/241 del Parlament Europeu i del Consell pel que s'establí el MRR. Norma directament aplicable a tots els estats membres des de la seva publicació al Diari Oficial de la UE.

D'aquesta manera, per poder accedir al MRR, l'estat espanyol va presentar un Pla de Recuperació, Transformació i Resiliència (en endavant, PRTR) aprovat pel Consell de la UE el 13 de juliol de 2021, a on recollia el conjunt d'inversions que es realitzaran i el programa de reformes previstes.

El programa RETECH constitueix un dels nous eixos transversals de l'Agenda España Digital 2026 promoguts pel Ministerio de Asuntos Económicos y Transformación Digital, i està aliniat amb dos de les principals fites de l'Agenda, com són, liderar la transformació digital de manera inclusiva i sostenible i focalitzar els esforços de digitalització en sectors econòmics clau. L'objectiu del Programa RETECH és impulsar xarxes territorials d'especialització tecnològica, articulant projectes regionals que s'orientin a la transformació i especialització digital, assegurant la coordinació la col·laboració i la complementaritat.

Gràcies a aquest nou eix de l'Agenda España Digital 2026, es pretén liderar un canvi disruptiu, de manera inclusiva i sostenible, focalitzant els esforços de digitalització en sectors econòmics clau. En definitiva, la iniciativa RETECH permetrà impulsar els projectes tractors proposats per les Comunitats i Ciutats Autònomes, fomentant l'intercanvi de coneixement i multiplicant les oportunitats de cada regió, a través de xarxes d'impacte nacional que permetin maximitzar l'equilibri territorial i la cohesió social entre elles.

Per fer efectiva la iniciativa RETECH amb total transparència i igualtat d'oportunitats per a totes les Comunitats i Ciutats Autònomes interessades, el Ministerio de Asuntos Económicos i Transformación Digital, a través de la Secretaria d'Estado de

Digitalització i Intel·ligència Artificial, va llançar una invitació pública destinada al seu desenvolupament de propostes de cooperació per finançar iniciatives emblemàtiques d'especialització territorial tecnològica dins de les seves competències.

El Component 15.17 (*Ciberseguretat: Enfortiment de les capacitats de Ciberseguretat de ciutadans, pimes i professionals; impuls de l'ecosistema del sector*) és el Component al qual s'ha de contribuir des de l'Agència de Ciberseguretat de Catalunya, i en concret els objectius CID 248 descrits a continuació:

Fita CID 248: Finalització dels projectes del programa d'impuls a la indústria de la Ciberseguretat nacional, del programa d'innovació en seguretat i de les accions connexes. Descripció: finalització dels projectes inclosos al Programa d'Impuls a la Indústria de la Ciberseguretat Nacional i al Programa Global d'Innovació en Seguretat, i altres accions connexes en els següents àmbits (adjudicats a la Fita 245 i a la Fita 453): - l'impuls de la indústria de ciberseguretat nacional amb vista al sorgiment, el creixement i el desenvolupament de noves empreses en aquest sector; - el desenvolupament de solucions i serveis d'elevat valor afegit a l'àmbit de la ciberseguretat; - la formació i capacitat de persones amb talent especialitzades en l'àmbit de la ciberseguretat; - les accions d'internacionalització a l'àmbit de la ciberseguretat; - la implantació d'un centre demostrador per al desenvolupament d'infraestructura de ciberseguretat i la creació de nous serveis de ciberseguretat, incloent-hi laboratoris d'assaig i simuladors de ciberatacs; - el desenvolupament de certificacions per a l'etiqueta de ciberseguretat.

Actualment, la Generalitat de Catalunya rep més de 7.000.000.000 atacs contra la seva infraestructura i sistemes d'informació, els quals en la majoria dels casos té com a objectiu posar en risc la disponibilitat, integritat i/o confidencialitat dels serveis públics de Catalunya.

Amb aquest context, és fonamental garantir les capacitats necessàries per poder realitzar una gestió eficient i eficaç davant aquesta activitat, identificant el més ràpid possible quina d'aquesta activitat és un incident potencial i requereix executar tasques de protecció o resposta per evitar l'afectació en processos crítics a la ciutadania. Per aquest fet, i amb l'objectiu de reduir els temps de detecció i resposta davant atacs i incidents de seguretat, aquest projecte persegueix desenvolupar automatitzacions de nivell 1 les quals, mitjançant els principals playbooks de gestió d'atacs i incidents de ciberseguretat, redueixen els temps de detecció, anàlisi i protecció de potencials ciberincidents, i incrementar de forma rellevant el grau de seguretat dels serveis públics de la Generalitat de Catalunya.

Per tot això, és imprescindible dotar l'Agència de Ciberseguretat d'un mecanisme/instrument de racionalització i eficiència en matèria de contractació. Aquest contracte ha de permetre alleugerir i simplificar la contractació, per tal de poder fer front, al més aviat possible, a la necessitat d'incorporar noves capacitats que pugui afrontar les ciberamenaces i el creixement exponencial de les exigències de suport que reclama el sector públic de Catalunya.

JUSTIFICACIÓ DEL PROCEDIMENT

El contracte s'adjudicarà per procediment basat en l'acord marc amb número d'expedient CB25AMOP2B002 de conformitat amb l'establert en l'article 222 i

següents de la LCSP. Addicionalment, el procediment d'adjudicació d'aquest contracte basat es farà seguint el següent procediment:

Contractació basada, nova licitació. En els casos de contractacions basades de quantia econòmica (valor estimat del contracte) superior al llindar econòmic establert en les directives europees de contractació (actualment, 221.000,00 euros), i de conformitat amb l'article 221.6 de la Llei de Contractes del sector públic, l'òrgan de contractació convidarà a totes les empreses homologades en el lot corresponent.

Aquest procediment es va publicar en l'annex 9 de l'Acord Marc de referència

La LCSP estableix unes consideracions generals en el seu article 131 de la LCSP i assenyala que, amb caràcter ordinari, l'adjudicació dels contractes es farà utilitzant una pluralitat de criteris d'adjudicació, sota el principi de millor relació qualitat/preu.

JUSTIFICACIÓ DE LA INSUFICIÈNCIA DE MITJANS

Es tracta de donar suport a diferents àrees de l'Agència de Ciberseguretat de Catalunya per a donar suport en l'optimització de l'eficiència i l'eficàcia dels serveis proporcionats per l'Àrea d'Operacions de la Seguretat mitjançant la industrialització dels processos, la seva automatització i l'actualització contínua de les solucions de Ciberseguretat.

És necessari poder fer aquesta contractació justificada en diferents aspectes:

1. Insuficiència de mitjans personals: funcions especialitzades que complementin i donin suport a les que realitza la plantilla de l'Agència. És necessari per a poder complir amb els projectes vigents suport en matèria d'evolució de les principals solucions transversals de l'àrea d'operacions.
2. Especialització amb l'objecte del contracte: L'objecte del basat és l'optimització de l'eficiència i l'eficàcia dels serveis proporcionats per l'Àrea d'Operacions de la Seguretat (AOS) de l'Agència de Ciberseguretat de Catalunya, el qual requereix una formació i especialització molt concreta per assolir els objectius i finalitats del servei.

Amb l'anàlisi realitzat es pot concloure que l'Agència de Ciberseguretat no consta amb els mitjans propis necessaris per a l'execució total de les tasques objecte d'aquest basat els processos de ciberseguretat requereixen un alt nivell d'especialització tècnica.

DIVISIÓ EN LOTS

D'acord amb el que es determina a l'article 99.3 de la Llei 9/2017 de Contractes del Sector Públic (LCSP), donada la naturalesa dels treballs objecte del contracte i per raons d'eficiència i economia no es considera oportú dividir el contracte en lots.

L'article 99.3 de la LCSP disposa el següent:

“3. Siempre que la naturaleza o el objeto del contrato lo permitan, deberá preverse la realización independiente de cada una de sus partes mediante su

división en lotes, pudiéndose reservar lotes de conformidad con lo dispuesto en la disposición adicional cuarta.

No obstante lo anterior, el órgano de contratación podrá no dividir en lotes el objeto del contrato cuando existan motivos válidos, que deberán justificarse debidamente en el expediente, salvo en los casos de contratos de concesión de obras.

La licitació per a la prestació de serveis d'automatització de processos de ciberseguretat no s'ha dividit en lots per les raons següents:

Naturalesa integral del servei:

L'automatització de processos de ciberseguretat és un servei que requereix una visió global i coordinada de totes les funcions de l'AOS. Dividir el projecte en lots podria generar duplicitats, manca de coherència en la implementació i dificultats d'integració entre les diferents parts del servei. Això afectaria negativament la qualitat i l'eficàcia de les solucions implantades.

Interdependència dels components:

Els diferents components de l'automatització de processos de ciberseguretat, com ara la gestió de riscos i de canvis, la prioritització de les tasques, el coneixement tècnic de les diferents eines i solucions, i l'execució i supervisió continuada dels evolutius, estan estretament interrelacionats. Separar aquests components en lots podria comprometre la coherència i la interoperabilitat del sistema de seguretat.

Optimització de recursos i coordinació:

Un únic proveïdor pot gestionar els recursos i les activitats de manera més eficient, evitant possibles conflictes o problemes de comunicació entre diferents adjudicataris. Això garanteix que el projecte es compleixi dins els terminis establerts i amb un enfocament uniforme.

Garantia de responsabilitat única:

L'adjudicació a un sol proveïdor assegura una línia de responsabilitat única, la qual cosa facilita la gestió contractual i assegura que qualsevol problema o incompliment pugui ser abordat de manera més efectiva.

Especialització requerida:

Els serveis d'automatització de processos de ciberseguretat requereixen un alt nivell d'especialització tècnica. Dividir en lots podria limitar la capacitat dels possibles licitadors per oferir un enfocament complet i cohesionat, ja que algunes empreses podrien no tenir experiència en tots els àmbits necessaris del servei.

Per les raons exposades, la no divisió de la licitació en lots assegura un millor resultat en termes de qualitat, eficàcia i seguretat, alineant-se amb els objectius estratègics i operatius del projecte.

DURADA DEL CONTRACTE

La durada del contracte serà fins al juny de 2026, per tant, compleix amb l'establert contracte en l'article 29 de la LCSP.

El conveni de RETECH especifica que el termini d'execució de la despesa conclourà el 30 de juny de 2026 a causa de la seva vinculació als Fons Next Generation, i als objectius i terminis del PRTR, per a aquelles actuacions que estiguin sota el marc del C15.eNo es preveuen prorrogues. e

CONSIDERACIONS ECONÒMIQUES

PRESSUPOST DE LICITACIÓ: S'entén per pressupost base de licitació el límit màxim de despesa que en virtut del contracte pot comprometre l'òrgan de contractació, inclòs l'Impost del Valor Afegit, excepte disposició en contrari.

El pressupost base de licitació ascendeix a 968.193,60 Euros (IVA inclòs) amb el següent desglossament:

Concepte	Import en Euros (IVA exclòs)	IVA en Euros (21%)	Import total en Euros (IVA inclòs)
Pressupost base de licitació	800.160,00	168.033,60	968.193,60

Aquest import ha estat calculat considerant l'estimació d'hores mínimes anuals que requereix aquest servei i que s'indica en el PPT, que és de 12.336 hores, i a raó d'un preu del perfil coordinador de l'automatització de 60,00€/h, del perfil enginyer d'automatització de 70,00€/h, i del perfil validador de seguretat de 60€/h. com a preus mitjans resultants de l'anàlisi de preus de mercat realitzat pels tres perfils.

VALOR ESTIMAT DEL CONTRACTE

S'entén per valor estimat del contracte el valor l'import total, sense incloure l'Impost del Valor Afegit, pagador segons les estimacions realitzades.

El mètode aplicat per calcular el valor estimat del contracte és, de conformitat amb l'article 101 de la LCSP, el següent: Preus de mercat en base a anteriors contractes de l'Agència de Ciberseguretat i d'altres entitats del sector públic.

El valor estimat del contracte ascendeix a la quantitat de 800.160,00Euros (IVA exclòs).

EXISTÈNCIA DE CRÈDIT

Existència de partida pressupostària	Disponible al Capítol 2 de Despesa
--------------------------------------	------------------------------------

S'annexa informe emès pel Director de l'Àrea de Serveis Corporatius on es posa de manifest l'existència de crèdit pressupostària.

QUALIFICACIÓ DE L'OBJECTE DEL CONTRACTE

Es qualifica com un contracte de serveis de conformitat amb el que estableix l'article 17 de la LCSP.

Els contractes de serveis son els que tenen per objecte prestacions consistents en el desenvolupament d'una activitat o que estan adreçats a l'obtenció d'un resultat diferent d'una obra o un subministrament. La LCSP inclou també com a contractes de serveis els contractes en els quals l'adjudicatari s'obliga a executar el servei de manera successiva i per preu unitari.

SOLVÈNCIA DE LES EMPRESES LICITADORES

La solvència és la mínima exigible en l'acord marc. Les empreses en el moment de la presentació de la oferta han de presentar declaració responsable inclosa en la documentació publicada en el perfil de contractant ratificant la solvència.

ADSCRIPCIÓ DE MITJANS PERSONALS

Perfils mínims necessaris per a l'execució del contracte

PERFIL	REQUISITS
Perfil coordinador de l'automatització	- Experiència professional mínima de 5 anys en gestió de projectes. - Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. - Certificat en: Project Management Professional (PMP), Certified Associate in Project Management (CAPM), PRINCE2 (Projects IN Controlled Environments), AgilePM, per part d'un integrant de l'equip. - Haver participat i poder demostrar la seva involucració en mínim un projecte en els que hagi desenvolupat les següents funcions: - Lideratge de projectes i equips de treball multidisciplinars. - Gestió i seguiment de projectes (incloent la identificació i validació de requeriments, gestió de riscos, identificació i control de desviaments de terminis, etc.) - Coneixements en: - Definició i millora de processos. - Gestió de projectes (metodologies, processos, eines, lliurables, etc.). - Eines de reporting i quadres de comandament. - Tecnologies aplicades a centres d'operació de la seguretat (SOCs).

	▪ Marcs metodològics més comuns de gestió (ITIL, ISO 20000, Prince2, COBIT, PMP o similar) i de seguretat (ISO27000, NIST o similar).
Perfil enginyer d'automatització	• Experiència professional mínima de 5 anys en projectes de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Especialista en Implementació i administració automatitzacions en eines SIEM/SOAR. • Certificat en: Palo Alto Networks Micro-Credential for Cortex XSOAR Consultant (PMXrC)) o Palo Alto Network Security Automation Engineer (PCSAE), per part d'un integrant de l'equip. • Haver participat i poder demostrar la seva involucració en mínim un projecte en els que hagi desenvolupat les següents funcions: ▪ Lideratge i gestió de projectes i equips de treball multidisciplinars. ▪ Gestió i operació de serveis de SOC. ▪ Projectes d'automatització i industrialització. ▪ Automatització de tasques operatives recurrents. ▪ Desenvolupament i consum d'APIs. ▪ Desenvolupament full stack multi plataforma. ▪ Desenvolupament de Backend WEB y API REST. • Coneixements en: ▪ Llenguatges de programació, especialment Python, Ruby, Javascript i Perl. ▪ Principals amenaces i vectors d'atac que afecten a les organitzacions (per exemple, el catàleg d'amenaces que proposa l'organització NIST). Habilitats comunicatives avançades i capacitat de coordinació i interlocució amb altres equips.
Perfil validador de seguretat	• Experiència professional mínima de 5 anys en projectes de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Coneixements tècnics en elements de seguretat, sistemes operatius, xarxes, protocols i programari. • Coneixements a nivell analític per abastar tot l'escenari d'un incident • Coneixements tècnics en investigació i anàlisi d'amenaces i atacs. • Coneixements tècnics dels elements de seguretat. • Coneixements relacionats amb l'aplicació de metodologies i operació d'eines de monitorització i protecció perimetral.

	• Coneixements per al tractament i resposta davant d'esdeveniments i incidents de seguretat.
--	--

CRITERIS D'ADJUDICACIÓ

OFERTA AVALUABLES MITJANÇANT L'APLICACIÓ DE CRITERIS SOTMESOS A UN JUDICI DE VALOR: fins a 49 punts

Per valorar cada un dels conceptes de la valoració subjectiva es tindran en compte els següents criteris:

- Comprensió dels requeriments. Profunditat i claredat de la proposta, que demostrï una clara comprensió de les característiques sol·licitades i el compliment dels requisits, i la seva superació, així com la identificació de possibles incerteses i les solucions proposades.
- Factibilitat i escalabilitat. Extensió en la que l'enfocament proposat és factible, adaptable i els resultats finals que es poden assolir.
- Completesa. Enfocament de la proposta en quant a completeness, considerant els diferents escenaris, mètodes i requisits.
- Exemplificació. Incloure exemples il·lustratius, que es poden aplicar a l'àmbit del present plec.
- Capacitat. Model de gestió de la capacitat, que regularà l'adaptació de la capacitat real d'execució dels serveis a les necessitats.
- Eficiència i eficàcia. Enfocament en la millora de l'eficiència i eficàcia en l'execució dels serveis, polivalència dels recursos, etc.
- Qualitat de la informació. Es valorarà la rellevància de la informació proporcionada, les fonts d'informació, el context i les tendències generals.
- Innovació. Es valorarà el grau d'innovació de les propostes per fer el servei més eficient, desplegant processos i eines d'automatització o industrialització.

Es puntuarà cada apartat dels continguts segons la següent taula:

Secció	Puntuació màxima
Solució tècnica proposada	20
Organització del servei	10
Gestió i transferència coneixement	5
Metodologia per al seguiment del servei	5
Aspectes crítics	9
Total	49

1. Solució tècnica proposada (fins a 20 punts):

En aquest apartat es valorarà principalment la comprensió dels serveis inclosos en el PPT, la completesa a l'hora de descriure i l'exposició d'experiències similars.

Es valorarà principalment els processos per l'execució dels serveis, processos operatius de suport, propostes de metodologies i eines de suport.

I addicionalment es valorarà la incorporació de la innovació dins els diferents processos i serveis propis, així com l'assoliment d'eficiències aportades per les propostes..

La pauta i paràmetre de valoració és el que es detalla a continuació:

- Processos per l'execució dels serveis: fins a un màxim de 9 punts
- Propostes de metodologies i eines de suport per a la execució del servei: fins a un màxim de 8 punts
- La innovació dins els diferents processos i serveis propis: fins a un màxim de 3 punts

2. Organització del servei (fins a un màxim de 10 punts)

En aquesta secció els licitadors han de descriure l'organització del servei, indicant els recursos assignats i les seves funcions per a fer front a la gestió dels projectes o activitats encomanades, així com el model de relació amb la resta de serveis i activitats de l'Agència.

Es valorarà el dimensionament i l'adequació de l'equip proposat (atenent pics i valls), a partir de l'equip mínim establert com a solvència, així com l'estructura del servei i la capacitat d'adaptació a la resta de serveis de l'Àrea i les accions encaminades a aconseguir una major integració i col·laboració entre tots els serveis que comportin una major eficiència del servei.

La pauta i paràmetre de valoració és el que es detalla a continuació:

- Estructura i organització de l'equip proposat per al servei: fins a un màxim de 4 punts.
- Escalabilitat i flexibilitat de l'equip del servei: fins a un màxim de 4 punts.
- Capacitat d'adaptació a la resta de serveis de l'Àrea: fins a un màxim de 2 punts

3. Gestió i transferència coneixement (fins a un màxim de 5 punts).

Mecanismes de gestió i transferència del coneixement que es generi durant la prestació dels serveis a favor de l'Agència de Ciberseguretat. Es valorarà el detall i valor dels mecanismes de gestió i transferència que assegurin un correcte traspàs.

- Mecanismes de gestió i transferència del coneixement. Fins a un màxim de 5 punts

4. Metodologia per al seguiment del servei (fins a un màxim de 5 punts).

En aquesta secció els licitadors han de descriure les metodologies, eines i recursos pel seguiment del servei,. Es valorarà l'adequació i detall d'aquests a les necessitats descrites en el PPT.

- Coherència i viabilitat de la metodologia. Fins a un màxim de 3 punts
- Processos de control de les capacitats internes i execució del servei. Fins a un màxim de 2 punts

5. Aspectes crítics (fins a 9 punts):

En aquesta secció els licitadors han d'enumerar i descriure quins són, segons el seu criteri, els quatre aspectes més crítics i significatius de les tasques que ha de dur a terme, per tal d'aconseguir els objectius del servei.

Es valorarà el detall i adequació dels aspectes crítics (fins un màxim de 3) identificats atenent als serveis descrits en el PPT així com la seva adequació al que s'exposa en el PPT respecte als objectius del servei d'arquitectura de seguretat. Cada aspecte crític identificat atorgarà un màxim de 3 punts.

CRITERIS AVALUABLES MITJANÇANT FÒRMULES O CIRTERIS AUOMÀTICS: fins a 51 punts

a. Valoració de l'oferta econòmica.....fins a 34 punts

En aquest apartat es valorarà la proposta econòmica.

La valoració econòmica es realitzarà tenint en compte l'estimació dels costos pels volums dels serveis descrits en el plec. Aquest serà Ov. Les ofertes amb un Ov (preu ofertat) calculat superior al pressupost de licitació quedaran excloses. La puntuació s'assignarà d'acord a la següent fórmula:

$$Pv = \left[1 - \left(\frac{Ov - Om}{IMR} \right) \times \left(\frac{1}{2} \right) \right] \times Pmax$$

On:

- Pv és la puntuació de l'oferta a valorar.
- Pmax és la puntuació màxima de l'apartat.
- Om és la millor oferta rebuda.
- Ov és la oferta a valorar.
- IMR és l'Import màxim

Criteris per a determinar la temeritat o desproporcionalitat de les ofertes

Es considerarà, en principi, que la proposició no pot ser acomplerta per temerària o desproporcionada quan l'oferta econòmica es trobi en algun dels següents supòsits:

Quan, concurrent un sol licitador, sigui inferior al pressupost base de licitació en més de 25 unitats percentuals.

Quan concorrin dos licitadors, la que sigui inferior en més de 20 unitats percentuals a l'altra oferta.

Quan concorrin tres licitadors, les que siguin inferiors en més de 10 unitats percentuals a la mitjana aritmètica de les ofertes presentades. Sens perjudici d'això, s'exclourà per al còmput de dita mitjana l'oferta de quantia més elevada quan sigui superior en més de 10 unitats percentuals a aquesta mitjana. En qualsevol cas, es considerarà desproporcionada la baixa superior a 25 unitats percentuals.

Quan concorrin quatre o més licitadors, les que siguin inferiors en més de 10 unitats percentuals a la mitjana aritmètica de les ofertes presentades. Sens perjudici d'això, si entre elles existeixen ofertes que siguin superiors a dita mitjana en més de 10 unitats percentuals, es procedirà al càlcul d'una nova mitjana només amb les ofertes que no es trobin en el supòsit indicat. En tot cas, si el nombre de les restants ofertes és inferior a tres, la nova mitjana es calcularà sobre les tres ofertes de menor quantia.

b. Grau de qualificació tècnica del perfil enginyer d'automatitzaciófins a 6 punts

Valorar aquelles certificacions que acreditin competències i coneixements els diferents àmbits d'especialització del perfil enginyer d'automatització permet a l'Agència atorgar valor a aquells equips que garanteixin un nivell de competència i professionalitat superior a la resta. Aquestes certificacions, assegurin que el perfil coneixen les metodologies estandarditzades, les bones pràctiques i les tecnologies associades que els permet donar un servei alineat amb els objectius definits en el plec tècnic. Finalment, aquesta exigència reforça la confiança en la qualitat i el valor del servei prestat.

Es valorarà el nivell de qualificació tècnica dels perfils enginyers d'automatització, en base al volum de certificacions de seguretat aportades. Es puntua 2 punts per cada certificació vàlida aportada.

Important: Només podrà aportar fins a un màxim de 3 certificacions, les que superin el número màxim prèviament esmentat no seran computades.

No es tindran en compte la certificació aportada com a requeriment tècnic al plec de prescripcions tècniques.

Només es valoraran les certificacions quan es compleixin amb els següents criteris:

Certificacions del següent llistat:

- Palo Alto Network Certified Security Operations Generalist,
- Palo Alto Networks (EDU-380) Cortex XSOAR,
- Palo Alto Network Security Automation Engineer (PCSAE),
- Palo Alto Networks Micro-Credential for Cortex XSOAR Consultant (PMXrC)

- Palo Alto Network Certified Detection and Remediation Analyst (PCDRA),
- Palo Alto Networks (EDU-260/2) Cortex XDR

Que el certificat estigui en vigor.

c. Experiència addicional

fins a 6 punts

Valorar aquesta experiència addicional que acrediti capacitats i coneixements en els diferents àmbits d'especialització del servei d'automatització de processos, permet a l'Agència atorgar valor a aquells equips que garanteixin un nivell de capacitats i professionalitat superior a la resta. Aquesta experiència reforça la confiança en la qualitat i el valor del servei prestat.

Es puntuarà fins un màxim de 2 punts a l'experiència en relació al perfil de coordinador de l'automatització addicional a la mínima indicada en el quadre resum per aquest perfil. Cada any d'experiència addicional al mínim requerit s'atorgarà un punt.

Es puntuarà fins un màxim de 2 punts a l'experiència en relació al perfil enginyer d'automatització addicional a la mínima indicada en el quadre resum per aquest perfil. Cada any d'experiència addicional al mínim requerit s'atorgarà un punt.

Es puntuarà fins un màxim de 2 punts a l'experiència en relació al perfil validador de seguretat addicional a la mínima indicada en el quadre resum per aquest perfil. Cada any d'experiència addicional al mínim requerit s'atorgarà un punt.

d. Suport amb hores de fabricant **5 punts**

fins a

Es puntuarà fins un màxim de 5 punts cada paquet de 20 hores extra a les 200 hores de suport del fabricant Palo Alto dels requisits, a raó d'1 punt per cada paquet de 20 hores de més, essent el màxim d'hores puntuables de 100 hores.

ALTRES CONSIDERACIONS DEL CONTRACTE

Responsable del contracte

D'acord amb el que estableix l'article 62 de de la LCSP, el responsable del contracte, al qual correspon supervisar-ne l'execució i adoptar les decisions i dictar les instruccions necessàries amb la finalitat d'assegurar la realització correcta de la prestació pactada, dins de l'àmbit de les facultats que l'òrgan de contractació li atribueix serà Pedro Lendinez, Director de l'Àrea SOC/CERT

De conformitat amb l'article 62 de la LCSP la unitat de seguiment del contracte es determinarà en cada contractació basada essent la direcció d'àrea competent per a cada contracte.

Condicions especials d'execució.

D'acord amb l'article 202 de la LCSP, es mencionen en el present document així com en el Plec de Clàusules Administratives.

a) Condició especial d'execució de caràcter social

Garantir la seguretat i prevenció de la salut en el lloc de treball

b) Condició especial d'execució de caràcter ètic

- Observar els principis, les normes i els cànons ètics propis de les activitats, i professions corresponents a les prestacions objecte del contracte.
- No realitzar accions que posin en risc l'interès públic
- Abstenir-se de realitzar conductes que tinguin per objecte o puguin produir l'efecte d'impedir, restringir o falsejar la competència, com els comportaments col·lusoris o la competència fraudulenta.
- Respectar els acords i les normes de confidencialitat.
- Col·laborar amb l'òrgan de contractació en les actuacions que aquest realitzi pel seguiment i/o avaluació del compliment del contracte, particularment facilitar 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, sense perjudici del compliment de les obligacions de transparència que els pertoqui de forma directa per previsió legal.

El Reglament 2021/241 del Parlament Europeu i del Consell, de 12 de febrer de 2021, pel qual s'estableix el Mecanisme de Recuperació i Resiliència i la resta de normativa que el desenvolupa, en particular es tindran en compte les mesures que preveu aquest reglament adreçades a:

- El compliment de les fites i objectius segons es disposa a l'annex I de l'ordre HFP/1030/2021, de 29 de setembre.
- L'aplicació dels percentatges de contribució climàtica i digital de les mesures, associats a la inversió 7 del component 15, on s'ha de complir en un 100% a l'etiquetatge digital
- evitar el doble finançament (article 9)
- les mesures contra el frau, la corrupció i el conflicte d'interessos (article 22.2.b)
- les mesures per al registre de les dades dels beneficiaris en una base de dades única (article 22.2.d)
- la subjecció als controls dels organismes europeus (article 22.2.e)
- l'obligació de conservació de la documentació (article 22.2.f)
- les normes sobre comunicació i publicitat, d'acord amb el que preveu l'article 34.

Tanmateix, l'empresa adjudicatària garantirà el respecte al principi de «no causar un perjudici significatiu als objectius medi ambientals» (DNSH), així com el compliment de la metodologia de seguiment de les ajudes d'acord amb el que preveu el PRTR, a l'article 5.2 del Reglament (UE) número 2021/241 del Parlament Europeu i del Consell de data 12 de febrer de 2021, i la seva normativa de desenvolupament i, en particular les vinculades al compliment de fites i objectius.

Revisió de preus

Aquest contracte no està subjecte a revisió de preus.

Termini de garantia

El termini de garantia es determinarà en les posteriors contractacions basades.

Cessió del contracte

De conformitat amb el que estableix l'article 214 de la LCSP, queda prohibida la cessió total o parcial dels drets i obligacions del contracte sense que hi hagi prèviament l'autorització de l'òrgan de contractació i sempre que les qualitats tècniques o personals de qui cedeix no hagin estat raó determinada per a l'adjudicació del contracte.

Penalitats

Les penalitats seran les determinades en l'article 193 de la LCSP, en el present plec de clàusules administratives particulars. En el cas que l'òrgan de contractació ho consideri necessari per l'objecte del contracte, aquestes es concretaran en els posteriors contractes basats prèvia justificació.

Garantia definitiva

Corresponent al 5% de l'import d'adjudicació

Altra informació

- *Presentació de les ofertes de forma **exclusivament electrònica**.*