MEMÒRIA JUSTIFICATIVA DE L'ACORD MARC DE SUBMINISTRAMENT DE SOLUCIONS I SERVEIS GESTIONATS DE SEGURETAT TIC (Exp. 1431-0003/2025)

De conformitat amb el que estableix l'article 116 de la Llei 9/2017, de 8 de novembre, de contractes del sector públic (LCSP), la subscripció de contractes per part de les administracions públiques requereix la tramitació prèvia de l'expedient corresponent, que ha d'iniciar l'òrgan de contractació motivant la necessitat del contracte. D'acord amb el que disposa l'article 28 de la LCSP, la naturalesa i extensió de les necessitats que es pretenen cobrir mitjançant el contracte projectat, així com la idoneïtat del seu objecte i contingut per satisfer-les, s'han de determinar amb precisió, i se n'ha de deixar constància en la documentació preparatòria, abans d'iniciar el procediment encaminat a la seva adjudicació.
Segons el mateix article 116, en l'expedient s'ha de justificar:

a) L'elecció del procediment de licitació.
b) La classificació que s'exigeixi als participants.
c) Els criteris de solvència tècnica o professional, i econòmica i financera, i els criteris que s'han de tenir en consideració per adjudicar el contracte (Segons l'article l'elecció de les fórmules s'ha de justificar en l'expedient), així com les condicions especials de la seva execució.
d) El valor estimat del contracte amb una indicació de tots els conceptes que l'integren, inclosos sempre els costos laborals si n'hi ha.
e) La necessitat de l'Administració que es vol satisfer mitjançant la contractació de les prestacions corresponents; i la seva relació amb l'objecte del contracte, que ha de ser directa, clara i proporcional.
f) En els contractes de serveis, l'informe d'insuficiència de mitjans.
g) La decisió de no dividir en lots l'objecte del contracte, si s'escau.

1. L'objecte de l'acord marc

L'objecte de l'acord marc és el subministrament, instal·lació i suport de productes i la prestació de serveis destinats a la seguretat TIC dels ens, organismes i entitats del sector públic local català.

L'acord marc es divideix en els lots següents:

Lot 1 – Solucions de seguretat TIC incloses al Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i la Comunicació (CPSTIC) del Centre Criptològic Nacional (CCN).

Lot 2 – Serveis d'auditoria tècnica de ciberseguretat.

Lot 3 – Serveis de gestió de la ciberseguretat.

Lot 4 – Serveis de Centre d'Operacions de Seguretat (SOC).

Lot 5 – Serveis d'adequació a l'Esquema Nacional de Seguretat (ENS).

Lot 6 – Serveis de formació i conscienciació en ciberseguretat ad-hoc.

Lot 7 – Serveis de CSIRT *(Computer Security Incident Response Team*).

No s'estableix cap límit pel que fa al nombre d'empreses amb què es subscriurà el lot 1, ni s'estableix cap límit pel que fa al nombre de llicències de fabricant. Una mateixa empresa pot presentar oferta de llicències de diferents fabricants. Les empreses licitadores hauran d'indicar

en la seva oferta els fabricants de les solucions que tinguin previst comercialitzar. Les empreses podran incorporar, posteriorment, altres fabricants que, en el moment de presentar l'oferta, no tinguin productes al llistat del CPSTIC, dintre de les famílies que l'empresa hagi ofert.

Els lot 2, 3, 4, 5, 6 es subscriuran amb un màxim de deu empreses (cada lot).

Els lots 4 i 7 es subscriuran amb un màxim de cinc empreses (cada lot).

L'objecte del contracte es detalla en el plec de prescripcions tècniques (PPT).

No s'està alterant l'objecte del contracte per evitar l'aplicació de les regles generals de contractació.

Codificació de l'objecte del contracte:

Lot 1 – Solucions de seguretat TIC incloses al CPSTIC:

CPV principal: 48000000-8 - Paquets de programes i sistemes d'informació

Altres CPV:
48730000-4 - Paquets de programes de seguretat
48900000-7 - Paquets de programes i sistemes informàtics diversos
32424000-1 - Infraestructura de xarxa
48931000-3 - Paquets de programes de formació
48200000-0 - Paquets de programes de gestió de xarxes, Internet i intranet
35710000-4 - Sistemes de comandament, control, comunicació i informàtics
32510000-1 - Sistema de telecomunicacions sense fil
32412000-4 - Xarxa de comunicacions
72212730-5 - Serveis de desenvolupament de programari de seguretat
48600000-4 - Paquets de programes de bases de dades i de funcionament
32200000-5 - Aparells transmissors de radiotelefonia, radiotelegrafia, radiodifusió i televisió
30232000-4 - Perifèrics
30211300-4 - Plataformes informàtiques
48510000-6 - Paquets de programes de comunicació
48800000-6 - Sistemes i servidors d'informació
30237280-5 - Accessoris d'alimentació elèctrica
30200000-1 - Equip i material informàtic

Lot 2 – Serveis d'auditoria tècnica de ciberseguretat:

CPV principal: 72000000-5 Serveis TI: consultoria, desenvolupament de programari, Internet i suport

Altres CPV: 72810000-1 Serveis d'auditoria informàtica
72220000-3 - Serveis d'assessorament en sistemes i consultoria tècnica

Lot 3 – Serveis de gestió de la ciberseguretat:

CPV principal: 72000000-5 Serveis TI: consultoria, desenvolupament de programari, Internet i suport

Altres CPV: 72510000-3 Serveis de gestió relacionats amb la informàtica
72810000-1 Serveis d'auditoria informàtica

Lot 4 – Serveis de SOC:

CPV principal: 72000000-5 Serveis TI: consultoria, desenvolupament de programari, Internet i suport

Altres CPV: 72222300-0 - Serveis de tecnologies de la informació
72600000-6 Serveis de suport informàtic i de consultoria

Lot 5 – Serveis d'adequació a l'ENS:

CPV principal: 72000000-5 Serveis TI: consultoria, desenvolupament de programari, Internet i suport

Altres CPV: 72600000-6 Serveis de suport informàtic i de consultoria
72212732-9 Serveis de desenvolupament de programari de seguretat de dades
72220000-3 - Serveis d'assessorament en sistemes i consultoria tècnica
72223000-4 - Serveis de revisió de les exigències de les tecnologies de la informació
72810000-1 - Serveis d'auditoria informàtica

Lot 6 – Serveis de formació i conscienciació en ciberseguretat *ad hoc*:

CPV principal: 80000000-4 - Serveis d'ensenyament i formació

Altres CPV: 80510000-2 Serveis de formació especialitzada
80550000-4 - Serveis de formació en seguretat

Lot 7 – Serveis de CSIRT:

CPV principal: 72000000-5 Serveis TI: assessorament, desenvolupament de programari, Internet i suport

Altres CPV: 72222000-7 - Serveis de planificació i revisió estratègica de sistemes d'informació o de tecnologies de la informació

2. Tipus de contracte:

L'acord marc es qualifica de subministrament: lot 1 —Solucions de seguretat TIC incloses al CPSTIC—, o de serveis: lots 2, 3, 4, 5, 6 i 7 —Serveis de ciberseguretat—, segons el que estableixen els articles 16 i 17 de la LCSP, per a la determinació de les normes que s'han d'observar en la seva adjudicació.

3. La necessitat i idoneïtat de l'acord marc:

L'acord marc és necessari per al compliment i la realització dels fins institucionals del Consorci Localret i especialment dels ens locals consorciats. La naturalesa i extensió de les necessitats que pretenen cobrir-se mitjançant l'acord marc projectat, així com la idoneïtat del seu objecte i contingut per satisfer-les, es concreten en racionalitzar la contractació de solucions i serveis gestionats de seguretat TIC.

4. El pressupost base de licitació i el valor estimat de l'acord marc:

El pressupost base de licitació, calculat segons una estimació del valor agregat total dels contractes basats en l'acord marc previstos, és de 20.100.000,00 d'euros, exclòs l'IVA (24.321.000,00 euros, inclòs l'IVA):

Lot 1 – Solucions de seguretat TIC incloses al CPSTIC:

Exclòs l'IVA	Inclòs l'IVA
6.000.000,00 €	7.260.000,00 €

Lot 2 – Serveis d'auditoria tècnica de ciberseguretat:

Exclòs l'IVA	Inclòs l'IVA
4.500.000,00 €	5.445.000,00 €

Lot 3 – Serveis de gestió de la ciberseguretat:

Exclòs l'IVA	Inclòs l'IVA
2.500.000,00 €	3.025.000,00 €

Lot 4 – Serveis de SOC:

Exclòs l'IVA	Inclòs l'IVA
2.500.000,00 €	3.025.000,00 €

Lot 5 – Serveis d'adequació a l'ENS:

Exclòs l'IVA	Inclòs l'IVA
2.500.000,00 €	3.025.000,00 €

Lot 6 – Serveis de formació i conscienciació en ciberseguretat ad-hoc:

Exclòs l'IVA	Inclòs l'IVA
1.500.000,00 €	1.815.000,00 €

Lot 7 – Serveis de CSIRT:

Exclòs l'IVA	Inclòs l'IVA
600.000,00 €	726.000,00 €

La quota corresponent actual de l'IVA és el 21 %.

El pressupost base de licitació, inclòs l'IVA, es desglossa de la manera següent:

Lot 1 – Solucions de seguretat TIC incloses al CPSTIC:

Costos directes	5.880.600,00 €
Costos indirectes	1.379.400,00 €
Despeses general (13 %)	943.800,00 €
Benefici industrial (6 %)	435.600,00 €

Total	7.260.000,00 €

Lot 2 – Serveis d'auditoria tècnica de ciberseguretat:

Costos directes		4.410.450,00 €
Costos indirectes		1.034.550,00 €
Despeses general (13 %)	707.850,00 €	
Benefici industrial (6 %)	326.700,00 €	
Total		5.445.000,00 €

Lot 3 – Serveis de gestió de la ciberseguretat:

Costos directes		2.450.250,00 €
Costos indirectes		574.750,00 €
Despeses general (13 %)	393.250,00 €	
Benefici industrial (6 %)	181.500,00 €	
Total		3.025.000,00 €

Lot 4 – Serveis de SOC:

Costos directes		2.450.250,00 €
Costos indirectes		574.750,00 €
Despeses general (13 %)	393.250,00 €	
Benefici industrial (6 %)	181.500,00 €	
Total		3.025.000,00 €

Lot 5 – Serveis d'adequació a l'ENS:

Costos directes		2.450.250,00 €
Costos indirectes		574.750,00 €
Despeses general (13 %)	393.250,00 €	
Benefici industrial (6 %)	181.500,00 €	
Total		3.025.000,00 €

Lot 6 – Serveis de formació i conscienciació en ciberseguretat ad-hoc:

Costos directes		1.470.150,00 €
Costos indirectes		344.850,00 €
Despeses general (13 %)	235.950,00 €	
Benefici industrial (6 %)	108.900,00 €	

Total	1.815.000,00 €

Lot 7– Serveis de CSIRT:

Costos directes	588.060,00 €
Costos indirectes	137.140,00 €
Despeses general (13 %)	94.380,00 €
Benefici industrial (6 %)	43.560,00 €
Total	726.000,00 €

El valor estimat del contracte, a efectes de determinar el procediment d'adjudicació, la publicitat i la competència de l'òrgan de contractació, d'acord amb el que estableix l'article 101 de la LCSP, calculant la seva durada inicial (2 anys), les pròrrogues eventuals del contracte (2 anys) i les modificacions previstes (clàusula trenta-vuitena del PCAP), és de 44.220.000,00 euros, exclòs l'IVA:

Lot 1 – Solucions de seguretat TIC incloses al CPSTIC:

Pressupost	Modificacions previstes	Possibles pròrrogues	Valor estimat
6.000.000,00 €	1.200.000,00 €	6.000.000,00 €	13.200.000,00 €

Lot 2 – Serveis d'auditoria tècnica de ciberseguretat:

Pressupost	Modificacions previstes	Possibles pròrrogues	Valor estimat
4.500.000,00 €	900.000,00 €	4.500.000,00 €	9.900.000,00 €

Lot 3 – Serveis de gestió de la ciberseguretat:

Pressupost	Modificacions previstes	Possibles pròrrogues	Valor estimat
2.500.000,00 €	500.000,00 €	2.500.000,00 €	5.500.000,00 €

Lot 4 – Serveis de Centre d'Operacions de Seguretat (SOC):

Pressupost	Modificacions previstes	Possibles pròrrogues	Valor estimat
2.500.000,00 €	500.000,00 €	2.500.000,00 €	5.500.000,00 €

Lot 5 – Serveis d'adequació a l'Esquema Nacional de Seguretat (ENS):

Pressupost	Modificacions previstes	Possibles pròrrogues	Valor estimat
2.500.000,00 €	500.000,00 €	2.500.000,00 €	5.500.000,00 €

Lot 6 – Serveis de formació i conscienciació en ciberseguretat ad-hoc:

Pressupost	Modificacions previstes	Possibles pròrrogues	Valor estimat
1.500.000,00 €	300.000,00 €	1.500.000,00 €	3.300.000,00 €

Lot 7 – Serveis de CSIRT(*Computer Security Incident Response Team*):

Pressupost	Modificacions previstes	Possibles pròrrogues	Valor estimat
600.000,00 €	120.000,00 €	600.000,00 €	1.320.000,00 €

El valor estimat és el valor màxim estimat exclòs l'IVA del conjunt de contractes basats previstos durant la vigència de l'acord marc: els efectes de l'acord marc s'esgotaran una vegada assolit aquest import (STJUE C-216/17).

5. La durada de l'acord marc:

L'acord marc tindrà una durada màxima de quatre anys, incloses les possibles pròrrogues, comptats des de l'endemà de la formalització o des de la data concreta que s'indiqui en el contracte:

a) Dos anys de durada inicial.

b) Dues pròrrogues d'un any. Les pròrrogues les acordarà l'òrgan de contractació i seran obligatòries per a les empreses, sempre que el seu preavís es produeixi almenys amb dos mesos d'antelació a la finalització del termini de durada de l'acord marc.

6. El procediment d'adjudicació:

L'adjudicació de l'acord marc es realitzarà mitjançant procediment obert, de conformitat amb el que estableix l'article 131.2 de la LCSP.

La utilització del procediment obert és lliure per a l'òrgan de contractació: tractant-se d'un procediment ordinari, no es requereix una especial justificació del procediment utilitzat per a l'adjudicació del contracte, sempre que es respectin les normes relatives a la forma d'utilització del mateix.

L'expedient es tramitarà de forma ordinària, sense reducció de terminis.

7. Les condicions d'aptitud i els criteris de solvència:

Raons d'índole tècnica i de garantia de l'execució de la prestació aconsellen l'habilitació empresarial, solvència econòmica i financera i tècnica o professional requerides en els plecs. Els criteris de capacitat i solvència que s'han fixat en els plecs són:

a) Solvència econòmica i financera

Les empreses licitadores hauran d'acreditar la solvència econòmica i financera, per mitjà d'un volum anual global de negocis mínim, referit al millor exercici dins dels tres últims disponibles en funció de les dates de constitució o d'inici d'activitats de l'empresari. El volum anual de negoci que han d'acreditar les empreses licitadores ha de ser almenys de:

- Lot 1 – Solucions de seguretat TIC incloses al CPSTIC: 500.000,00 euros.

- Lots 2, 5, 6 i 7 – Serveis de ciberseguretat: 100.000,00 euros.

- Lots 3 i 4 – Serveis de ciberseguretat: 300.000 euros.

El requeriment de solvència econòmica i financera té caràcter selectiu.

b) Solvència tècnica o professional:

Les empreses licitadores hauran d'acreditar:

- Lot 1 – Solucions de seguretat TIC incloses al CPSTIC:
  - Haver efectuat un mínim de cinc subministraments de la mateixa o similar naturalesa als que constitueixen l'objecte del contracte en el curs de, com a màxim, els tres últims anys, l'import acumulat dels quals sigui igual o superior als 200.000,00 euros.
- Lots 2 – Serveis d'auditoria tècnica de ciberseguretat:
  - Haver efectuat un mínim de cinc serveis de la mateixa o similar naturalesa als que constitueixen l'objecte del contracte en el curs de, com a màxim, els tres últims anys, l'import acumulat dels quals sigui igual o superior als 100.000,00 euros.
  - ISO 27001, en matèria de seguretat de la informació.
- Lots 3 – Serveis de gestió de la ciberseguretat:
  - Haver efectuat un mínim de cinc serveis de la mateixa o similar naturalesa als que constitueixen l'objecte del contracte en el curs de, com a màxim, els tres últims anys, l'import acumulat dels quals sigui igual o superior als 200.000,00 euros.
- Lots 4 – Servei de SOC:
  - Haver efectuat un mínim de cinc serveis de la mateixa o similar naturalesa als que constitueixen l'objecte del contracte en el curs de, com a màxim, els tres últims anys, l'import acumulat dels quals sigui igual o superior als 200.000,00 euros
- Lots 5 – Servei d'adequació de l'ENS:
  - Haver efectuat un mínim de cinc serveis de la mateixa o similar naturalesa als que constitueixen l'objecte del contracte en el curs de, com a màxim, els tres últims anys, l'import acumulat dels quals sigui igual o superior als 100.000,00 euros.
  - ISO 27001, en matèria de seguretat de la informació.
- Lots 6 – Servei de formació i conscienciació en ciberseguretat ad-hoc:
  - Haver efectuat un mínim de cinc serveis de la mateixa o similar naturalesa als que constitueixen l'objecte del contracte en el curs de, com a màxim, els tres últims anys, l'import acumulat dels quals sigui igual o superior als 100.000,00 euros.
- Lots 7 – Servei de CSIRT:
  - Haver efectuat un mínim de cinc serveis de la mateixa o similar naturalesa als que constitueixen l'objecte del contracte en el curs de, com a màxim, els tres últims anys, l'import acumulat dels quals sigui igual o superior als 100.000,00 euros.
  - ISO 27001, en matèria de seguretat de la informació.

Tots els criteris seleccionats estan vinculats a l'objecte del contracte, són proporcionals al mateix, i es preveuen als articles 87 a 91 de la LCSP; no perjudiquen la competitivitat ni restringeixen injustificadament la concurrència de les empreses: s'han dissenyat per facilitar, en particular, la participació de les petites i mitjans empreses (pimes).

8. Els criteris d'adjudicació de l'acord marc:

L'adjudicació dels contractes s'ha d'efectuar utilitzant una pluralitat de criteris d'adjudicació sobre la base de la millor relació qualitat-preu.

La millor relació qualitat-preu s'avaluarà d'acord amb criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor i criteris d'adjudicació quantificables a través de la mera aplicació de fórmules.

Pel que fa als criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor, es tindrà en compte l'ordre, la claredat, la coherència, i la concreció de la proposta presentada. No es valoraran les ofertes que no es formulin amb claredat, segons l'índex proposat, i no estiguin suficientment desenvolupades. No es valorarà la informació que no figuri expressament a l'oferta, no sent suficient la remissió a informació externa; per exemple, a través d'enllaços, ni tampoc remissions genèriques a la informació que figura en els plecs

Lot 1 – Solucions de seguretat TIC incloses en el CPSTIC:

No s'estableixen criteris d'adjudicació, considerant que no s'estableix cap límit quant al nombre d'empreses amb què es subscriurà el lot 1, ni tampoc s'estableix cap límit quant al nombre de llicències de fabricant.

Lot 2 – Serveis d'auditoria de la ciberseguretat:

Criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor, fins a un màxim de 65 punts:

1. Anàlisi de l'entitat, fins a un màxim de 45 punts:

   Es valorarà la metodologia (tècniques, eines i procediments) i el nivell d'anàlisi de l'auditoria tècnica de ciberseguretat:

   Subcriteris:

1.1. Eines tècniques i procediment, fins a un màxim de 15 punts:

   Es valorarà la metodologia (tècniques, eines i procediments) específica emprada per auditar els sistemes informàtics, les aplicacions crítiques i la infraestructura de xarxes de l'entitat; en concret, la capacitat per identificar vulnerabilitats tècniques de seguretat (com configuracions incorrectes, falta de pedaços i accessos no controlats) i l'avaluació de la seva robustesa davant possibles atacs de ciberseguretat.

1.2. Abast i nivell de detall de l'auditoria, fins a un màxim de 15 punts:

   Es valorarà l'abast i nivell de detall de l'auditoria en relació amb, entre altres, els sistemes, aplicacions, xarxes, inventariat d'equips i d'usuaris, desenvolupament d'aplicacions pròpies, identificació de riscos, exposició de les dades de caràcter personal i el pla de seguretat; així com també l'anàlisi de la governança de ciberseguretat, pel que fa a mesures organitzatives i legals presents en els entorns de l'entitat i el treball de camp emprat per a tal finalitat.

1.3. Vectors d'atac i identificació de riscos, fins a un màxim de 15 punts:

   Es valoraran els vectors d'atac utilitzats per a la determinació de la robustesa dels sistemes, que abordin tots els aspectes crítics de la seguretat dels mateixos (físics,

digitals i humans), amb un enfocament innovador i adaptat específicament a l'entitat corresponent.

Es valorarà l'ús de *exploits zero-day* o altres tècniques avançades, així com la capacitat d'integrar nous vectors d'atac basats en tendències recents del sector.

Es tindrà en compte, especialment, la claredat i el detall en la descripció de les proves realitzades, l'adaptabilitat de les tècniques als processos i fluxos operatius de l'entitat i la capacitat d'evitar interrupcions en el funcionament normal dels sistemes durant les proves.

Justificació del criteri:

En l'anàlisi de l'auditoria cal una valoració dels diferents components dels sistemes d'informació i la seva seguretat, així com de la seva governança:

- Sistemes, aplicacions i xarxes.
- Equips i usuaris.
- Dades de caràcter personal.

L'auditoria ha de realitzar un anàlisi complert de tots els components dels sistemes d'informació de l'entitat. Un abast profund de la xarxa redundarà en major garantia en la seguretat integral d'aquesta xarxa. No seria coherent fer una auditoria parcial dels sistemes deixant forats de seguretat desconeguts per l'entitat.

La auditoria ha de valorar la robustesa de tots els elements de la xarxa i garantir que pot descobrir totes les vulnerabilitats de l'entitat en matèries de ciberseguretat. Atès que les vulnerabilitats no són conegudes en el moment de la licitació, sinó que es van descobrint cada dia, cal que la licitadora garanteixi que el seu servei evoluciona a mesura que apareixen aquestes vulnerabilitats, o que la tecnologia utilitzada compta amb les capacitats necessàries per descobrir els riscos potencials del sistema d'informació de l'entitat en el seu conjunt.

2. Documentació a lliurar, fins a un màxim de 20 punts:

Es valorarà la qualitat dels lliurables (informe final de l'auditoria i informe executiu); en concret, l'estructura, format, organització, personalització i alineament amb les necessitats del servei (per exemple, que incloguin exemples pràctics o escenaris reals de les vulnerabilitats).

Justificació del criteri:

Els informes contindran el resultat del servei, és on cal recollir tota la informació que s'hagi pogut extreure de l'auditoria. Aquests informes han de ser exhaustius amb el resultat del sistema analitzat, però alhora han de poder ser interpretats pels seus destinataris, que tot i ser tècnics informàtics no són necessàriament experts en ciberseguretat. Addicionalment l'entitat haurà de valorar amb l'anàlisi dels documents quina ha de ser la priorització de tasques i la inversió econòmica que ha de realitzar proporcionant un camí clar per a la resolució de les vulnerabilitats detectades. Per tant, aquí la claredat dels documents és tan important com el contingut en sí mateix.

Criteris d'adjudicació quantificables mitjançant la mera aplicació de fórmules, fins a un màxim de 35 punts:

3. Durada del suport post-auditoria, fins a un màxim de 10 punts:

Es valorarà ampliar la durada del suport post-auditoria per a la resolució de problemes detectats a l'informe (apartat 5.2 del PPT).

El temps mínim de suport post-auditoria és de 2 mesos (apartat 5.2 del PPT). Les empreses poden oferir un termini màxim de suport post-auditoria de 4 mesos.

Fórmula:

$$\mathrm{P} = 10 * \frac{(\text{dies de suport ofert} - 120)}{(240 - 120)}$$

Justificació del criteri:

Un cop realitzada l'auditoria, l'entitat contractant haurà de portar a terme la resolució dels problemes detectats a l'informe: el suport de l'empresa durant el màxim període de temps garanteix que l'entitat pugui abordar aquestes millores amb l'ajuda de l'auditor.

4. Pla de formació, 10 punts:

Es valorarà el compromís de les empreses licitadores d'incloure en el servei d'auditoria una proposta de pla de formació en ciberseguretat, adaptat als resultats de l'auditoria, segons les vulnerabilitats i riscos detectats.

Justificació del criteri:

El resultat de l'auditoria tècnica ha de ser un full de ruta per l'entitat per abordar millores en els seus sistemes d'informació per augmentar la seva seguretat.

Un pla de formació personalitzat, basat en els resultats de l'auditoria tècnica, assegura que els tècnics de l'entitat tinguin la capacitació necessària per entendre les mancances del seu sistema i abordar les millores que plantegi el resultat de l'auditoria tècnica: optimització de recursos, mitigació de riscos, millorar la cultura de seguretat i assegurar el compliment de la normativa vigent així com les bones pràctiques, entre d'altres.

5. Lloc de realització de l'auditoria, 10 punts:

Es valorarà el compromís de que els serveis d'auditoria es realitzin (presencialment) a les dependències de l'ens contractant en un 20 % del temps de dedicació, sempre que l'ens contractant així ho requereixi.

Justificació del criteri:

Les auditories amb visites presencials podran assegurar l'accés a tots els sistemes i l'entorn auditat amb una millor detecció de vulnerabilitats i riscos. També permetran comprovar la seguretat física i operativa, com el control d'accés físic o la seguretat en dispositius.

La realització del 80 % de l'auditoria en remot permet tenir un equilibri entre l'eficàcia i l'optimització de recursos.

6. Termini d'entrega dels informes, fins a un màxim de 5 punts:

Es valorarà que el termini de lliurament de l'informe final d'auditoria, un cop finalitzada la fase de recollida de dades, sigui inferior a 7 dies laborables, amb un temps mínim d'un dia laborable).

Fórmula:

$$P = 5 * \frac{\text{Temps màxim permès (7 dies)}}{\text{Temps ofert pel licitador (en dies} - \text{mínim 1 dia)}}$$

Justificació del criteri:

Un cop realitzada l'auditoria és convenient traslladar ràpidament el resultat a l'entitat perquè pugui actuar possible amb celeritat i així solucionar qualsevol dels forats de seguretat que pugui tenir.

Lot 3 – Serveis de gestió de la ciberseguretat:

Criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor, fins a un màxim de 65 punts:

1. Funcionalitats, fins a un màxim de 55 punts:

   Subcriteris:

1.1. Identificació i anàlisi d'actius, fins a un màxim de 15 punts:

   Es valorarà la millor idoneïtat del servei per identificar i analitzar els actius de l'entitat, així com per determinar el seu estat de compliment en matèria de seguretat, la exhaustivitat de l'anàlisi i la claredat i detall dels processos descrits per avaluar el compliment.

1.2. Manteniment, fins a un màxim de 15 punts:

   Es valorarà l'abast i periodicitat de la proposta de manteniment per garantir la seguretat dels actius de l'entitat.

1.3. Gestió d'amenaces i alertes, fins a un màxim de 15 punts:

   Es valorarà la millor idoneïtat del servei per gestionar amenaces i alertes de manera efectiva.

1.4. Resposta a incidents, fins a un màxim de 10 punts:

   Es valoraran el nivell de detall i adequació de les funcions operatives i la capacitat del servei per oferir respostes ràpides i coordinades davant incidents de seguretat.

   Justificació del criteri:

   En un servei de gestió de la ciberseguretat, l'avaluació de les funcionalitats que aborden la seguretat de les operacions resulta essencial per garantir una protecció eficaç i adaptada als actius i necessitats de l'entitat. Els aspectes valorats en aquest criteri cobreixen els elements essencials per a la detecció, gestió i resposta davant incidents de seguretat, així com per al manteniment de la continuïtat operativa.

   Aquest criteri de valoració garanteix que el servei de ciberseguretat ofert no només inclou les funcionalitats bàsiques, sinó que també proporciona eines per a una protecció adaptada, proactiva i continuada de l'entitat, alineada amb les millors

pràctiques i enfocada a la prevenció i la continuïtat operativa en cas de detectar amenaces i alertes o patir un incident.

2. Organització del servei, fins a un màxim de 10 punts:

   Es valorarà la descripció de l'estructura organitzativa dels perfils del servei de gestió de ciberseguretat (clàusula 6.2 del PPT), l'explicació dels perfils i les seves funcions concretes, així com l'eficiència de l'organització del servei.

   Justificació del criteri:

   La valoració de l'organització del servei és essencial per assegurar que l'empresa adjudicatària posseeixi una estructura clara i eficient, amb personal qualificat i processos ben definits per al desenvolupament i seguiment del servei.

   Una estructura organitzativa ben definida garanteix que les funcions i responsabilitats estan clarament delimitades, evitant redundàncies i buits de cobertura.

   Aquest criteri de valoració permet garantir que l'empresa adjudicatària ofereixi un servei de ciberseguretat ben estructurat, amb personal qualificat i un seguiment continu que asseguri l'eficàcia, la qualitat i l'adaptabilitat del servei a les necessitats de l'entitat.

Criteris d'adjudicació quantificables mitjançant la mera aplicació de fórmules, fins a un màxim de 35 punts:

3. Temps de resposta presencial, fins a un màxim de 15 punts:

   Es valorarà el temps que l'empresa trigarà en desplaçar-se físicament a les instal·lacions de l'entitat contractant, en cas d'incidència que requereixi intervenció presencial.

   Fórmula:

$$\mathrm{P} = 15 * \frac{\text{Temps mínim entre les propostes (mínim, 1 h)}}{\text{Temps proposat (màxim, 4 h)}}$$

   Justificació del criteri:

   La capacitat de l'adjudicatari per desplaçar un equip a les dependències de l'entitat contractant de manera ràpida, és un requisit crític per a la resposta efectiva davant incidents de ciberseguretat que puguin afectar la continuïtat operativa o la seguretat de la informació. Aquest criteri de valoració s'estableix amb l'objectiu de garantir que l'entitat pugui comptar amb suport presencial immediat en situacions d'emergència o de risc elevat.

4. Temps de resposta i resolució d'incidències de criticitat alta, fins a un màxim de 15 punts:

   Es valorarà el temps total requerit per identificar, diagnosticar i resoldre incidències de criticitat alta.

   Fórmula:

$$\mathrm{P} = 15 * \frac{240 \text{ minuts (Temps màxim permès)}}{\text{Temps proposat (mínim, 60 minuts)}}$$

Justificació del criteri:

La reducció del temps de resposta i resolució d'incidències de criticitat alta reduirà també l'afectació de la incidència al funcionament dels sistemes d'informació de l'entitat que ha patit l'incident.

Aquest criteri de valoració assegura que l'adjudicatari ofereix no només un servei tècnic de qualitat sinó també una capacitat de resposta ràpida en moments crítics, oferint així una seguretat proactiva i eficient davant qualsevol imprevist de ciberseguretat.

5. Eina de ticketing, 5 punts:

Es valorarà que el licitador ofereixi accés a l'entitat contractant a una eina de ticketing per al registre, el control i el seguiment de l'activitat.

Justificació del criteri:

Les eines de ticketing són importants perquè obren un canal de comunicació directe entre l'adjudicatari i l'entitat contractant, estalviant temps a tots dos i permetent a l'entitat la traçabilitat de les incidències del servei.

Lot 4 – Serveis de SOC:

Criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor, fins a un màxim de 45 punts:

1. Funcions i capacitats del SOC, fins a un màxim de 30 punts:

Es valoraran les funcions del servei SOC proposat: prevenció, detecció, protecció i resposta a incidents:

1.1. Capacitats de prevenció, fins a un màxim de 10 punts:

Es valorarà la millor idoneïtat de la solució per anticipar amenaces, gestionar vulnerabilitats i analitzar la superfície d'exposició de l'entitat, segons els següents paràmetres:

- Informes d'inventari i classificació d'actius segons la seva criticitat.
- Eines utilitzades per a l'anàlisi i gestió de vulnerabilitats, amb especial èmfasi en els escanejos de vulnerabilitats, proves tècniques com *pentests* i tests de *phishing*.
- Propostes concretes per al seguiment i mitigació d'aspectes identificats a la superfície d'exposició externa.

1.2. Capacitats de detecció, fins a un màxim de 10 punts:

Es valorarà la millor idoneïtat per a la detecció d'amenaces mitjançant monitorització 24x7 i ús de tecnologies avançades com SIEM/XDR, segons els següents paràmetres:

- Regles de detecció desenvolupades per mitigar amenaces concretes.
- Implementar anàlisi proactiu d'amenaces amb pràctiques de Threat Hunting.
- Creació de quadres de comandament en temps real que ofereixin visibilitat de les amenaces i indicadors de compromís.

1.3. Capacitats de protecció, fins a un màxim de 5 punts:

Es valorarà l'aplicació de contramesures i operació de les eines de protecció, mitjançant els següents punts:

- Desplegament de contramesures efectives en incidents simulats o reals.
- Nivell d'automatització de les tasques recurrents per evitar errors humans i millorar la rapidesa de resposta.

1.4. Resposta a incidents, fins a un màxim de 5 punts:

Es valorarà la millor idoneïtat per a la resposta a incidents, segons els següents paràmetres:

- La implementació d'anàlisis forenses i coordinació amb el SOC Tàctic en incidents crítics.
- Seguiment de la cadena de custòdia de les evidències recopilades.

Justificació del criteri:

Els serveis SOC (Centre d'Operacions de Seguretat) són crucials per prevenir, detectar, protegir i respondre a incidents de seguretat en temps real, garantint així la resiliència i la continuïtat de les operacions de l'entitat.

Aquest criteri de valoració garanteix que el SOC disposi de les capacitats necessàries per gestionar la seguretat de manera integral, des de la prevenció fins a la resposta davant incidents. La descripció detallada d'aquestes funcions assegura que el servei es presta amb un alt nivell de qualitat, amb alta capacitat reactiva i una orientació proactiva i de millora contínua per garantir la seguretat de l'entitat.

2. Prestacions tècniques del SIEM, fins a un màxim de 10 punts:

Es valoraran les automatitzacions i correlacions a implantar en el SIEM, així com la inclusió d'elements que facilitin la integració amb les eines de l'ecosistema del Centre Criptològic Nacional i l'enviament de trànsit de xarxa de manera selectiva a aquestes.

Justificació del criteri:

La descripció tècnica detallada de l'arquitectura permet assegurar que el SIEM proposat proporciona garanties sobre l'eficàcia, la seguretat i la sostenibilitat de la solució a implementar, i que pot detectar incidents i correlacionar esdeveniments de manera efectiva, adaptant-se a les necessitats específiques de l'entitat contractant.

La valoració de les funcionalitats d'integració amb les eines del CCN és essencial per assegurar que el SIEM pot interactuar de manera fluida amb el Centre Criptogràfic Nacional (CCN).

3. Implantació del SOC, fins a un màxim de 5 punts:

Es valorarà la millor idoneïtat per analitzar i adaptar-se a la infraestructura de l'entitat, mitjançant la concreció de la proposta de processos, procediments i estratègia d'implantació.

Justificació del criteri:

La valoració de la implantació del SOC té com a objectiu assegurar que l'adjudicatària ofereix una proposta ben estructurada, planificada i adaptada a les necessitats i particularitats de l'entitat contractant. Un procés d'implantació clar i detallat és

essencial per garantir que el SOC es desplega de manera eficient, coherent amb les infraestructures existents, i que cobreix tots els aspectes crítics de la seguretat.

Aquest criteri de valoració permet garantir que la implantació del SOC sigui executada amb un enfocament integral i ben planificada. Una metodologia clara, amb una estructura de fases, anàlisi d'infraestructura i eines adequades, assegura que el SOC compleixi plenament amb les expectatives i ofereixi un servei robust de ciberseguretat, capaç de protegir de manera eficient l'entitat contractant.

Criteris d'adjudicació quantificables mitjançant la mera aplicació de fórmules, fins a un màxim de 55 punts:

4. Temps d'instal·lació i gestió d'un SIEM, fins a una màxim de 15 punts:

   Es valorarà el temps d'instal·lació d'un sistema de gestió d'esdeveniments i incidència de seguretat (SIEM) per a la monitorització continuada de la seguretat del sistema, així com la seva configuració i posada en funcionament.

   Fórmula:

$$P = 15 * \frac{15 \text{ dies naturals} - \text{Temps d'instal} \cdot \text{lació ofert (dies naturals)}}{15 \text{ dies naturals} - \text{Temps mínim d'instal. lació (5 dies naturals)}}$$

   El temps per a la instal·lació i posta en marxa del SIEM no podrà superar els 15 dies naturals i tampoc no podrà ser inferior a 5 dies naturals.

   Justificació del criteri:

   La delimitació del temps d'instal·lació i posta en marxa d'un SIEM garanteix un ràpid inici de la protecció de l'entitat contractant. La capacitat del licitador de posar en marxa un SIEM significa addicionalment que és coneixedor de l'eina i aportarà un valor afegit més alt a la gestió de la mateixa.

5. Generació d'informes d'incidències, 15 punts:

   Es valorarà el compromís de redactar un informe setmanal que reculli les incidències més destacables d'aquest període i les vulnerabilitats observades, amb propostes d'accions correctores.

   Justificació del criteri:

   La realització d'un seguiment setmanal del servei ofert permetrà a l'entitat contractant actuar més ràpidament per reduir les vulnerabilitat trobades i posar en marxa les propostes correctores amb anticipació als incidents reduint així el seu risc de patir un ciberincident.

6. Generació d'informes post-incident, 15 punts:

   Es valorarà el compromís de redactar un informe post-incident detallat que inclogui l'anàlisi de l'incident amb la seva descripció, impacte, anàlisis de les causes, propostes d'accions correctores i mesures preventives i mitigadores aplicades.
   Justificació del criteri:

   La informació obtinguda en la resolució d'un incident és important per evitar la seva repetició. Cal conèixer quin ha estat el seu abast, les causes i quines accions es poden

portar a terme per tal de solucionar a vulnerabilitat existent en el moment de l'incident. Una documentació de l'incident és molt important per evitar la seva repetició.

7. Temps de resposta i resolució d'incidències no crítiques, fins a un màxim de 10 punts:

Es valorarà el temps total requerit per identificar, diagnosticar i resoldre incidències no crítiques. El temps mínim permès és 1 hora.

Fórmula:

$$P = 10 * \frac{24 \text{ h (Temps màxim permès)}}{\text{Temps proposat (mínim, 1h)}}$$

Justificació del criteri:

La reducció del temps de resposta i resolució d'incidències no crítiques reduirà l'afectació de la incidència al funcionament dels sistemes d'informació de l'entitat que ha patit l'incident.

Aquest criteri de valoració assegura que l'adjudicatari ofereix no només un servei tècnic de qualitat sinó també una capacitat de resposta ràpida, afavorint una seguretat proactiva i eficient davant qualsevol imprevist de ciberseguretat.

Lot 5 – Serveis d'adequació a l'ENS:

Criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor, fins a un màxim de 50 punts:

1. Governança de la seguretat, fins a un màxim de 25 punts:

Es valorarà la millor idoneïtat de la proposta en relació amb la gestió de la governança del servei, així com els mecanismes per assegurar l'adequació al marc normatiu.

Justificació del criteri:

El criteri de "Governança de la seguretat" permet avaluar la capacitat del licitador per establir una estructura de gestió sòlida i orientada al compliment continuat dels requisits de seguretat. Aquesta valoració és essencial per garantir que els serveis contractats es gestionaran de manera eficient i que l'adjudicatària aplicarà un control efectiu per assegurar el compliment dels estàndards de seguretat en el temps.

Aquest criteri és clau per garantir que l'adjudicatària no només implementi un sistema de seguretat, sinó que mantingui una gestió proactiva i estratègica del compliment normatiu i operatiu en el temps. Una governança efectiva i ben estructurada proporciona la garantia de que la seguretat estarà en constant revisió i ajust, contribuint a la confiança i sostenibilitat del servei.

2. Acompanyament a l'obtenció de la conformitat amb l'ENS, fins a un màxim de 25 punts:

Es valorarà l'acompanyament per a l'obtenció de la conformitat amb l'ENS i l'ajuda en les gestions amb l'empresa certificadora en la fase d'auditoria, així com la resolució de les possibles no-conformitats aparegudes.

Justificació del criteri:

Aquest criteri permet avaluar la capacitat del licitador per guiar l'entitat contractant en tot el procés d'obtenció de la conformitat amb les normatives de seguretat, assegurant que es compleixen tots els requisits exigits. L'acompanyament en la conformitat és un aspecte essencial per a la correcta implementació i certificació dels sistemes de seguretat, especialment en administracions públiques, on el compliment normatiu és crític.

Criteris d'adjudicació quantificables mitjançant la mera aplicació de fórmules, fins a un màxim de 50 punts:

3. Eina repositori, 25 punts:

Es valorarà el compromís d'aportar una eina repositori de la documentació necessària per a l'adequació a l'ENS. Aquesta eina haurà de complir les següents funcions:

- Organitzar la classificació i l'accés a tota la informació requerida.
- Ser guia metodològica sobre els passos i requisits per a l'adequació a l'ENS.
- Accés a documentació rellevant per a l'adequació normativa a l'ENS.

Justificació del criteri:

L'eina repositori de documentació permet a l'entitat visualitzar de manera ordenada i conjunta la seva evolució en l'adequació a l'ENS. L'aportació de models de la documentació ja personalitzats pel tipus d'entitat que demanda el servei estalvia temps en l'elaboració d'aquests documents.

4. Auditories internes, 25 punts:

Es valorarà el compromís de realitzar tres auditories internes durant els dos anys compresos entre les auditories regulars ordinàries, amb l'objectiu de verificar el correcte compliment de l'ENS i el manteniment de les mesures implementades.

Justificació del criteri:

Amb aquest criteri es persegueix avaluar el grau de compromís del licitador envers l'entitat contractant al llarg de la vida de la certificació de l'ENS, facilitant així el manteniment del nivell assolit i la verificació de la correcta aplicació de les mesures aplicades.

Amb la periodicitat prevista es busca espaiar en períodes racionals les auditories i abastar així el temps entre adequacions. Així, l'entitat comptarà amb els mecanismes degudament actualitzats i facilitarà la següent adequació i consecució del nivell de l'ENS.

Lot 6 – Serveis de formació i conscienciació en ciberseguretat ad-hoc:

Criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor, fins a un màxim de 45 punts:

1. Proposta formativa, fins a un màxim de 30 punts:

Es valorarà la proposta formativa per als empleats municipals: cursos proposats, temari per a completar la formació, durada de les formacions i programació de les sessions.

Justificació del criteri:

Aquest criteri permet avaluar l'adequació i qualitat del programa formatiu proposat per l'empresa licitadora en matèria de ciberseguretat. La formació i conscienciació en ciberseguretat són elements fonamentals per a qualsevol organització, ja que els errors humans sovint representen una de les vulnerabilitats més importants. La descripció dels nivells de formació en termes de temàtica i composició d'àrees assegura que el programa cobreixi un ampli ventall de coneixements i habilitats adaptats a diferents perfils dins de l'organització, millorant la capacitat de resposta i prevenció de tots els membres.

2. Orientació a l'entitat contractant i formació a mida del nivell avançat, fins a un màxim de 15 punts:

Es valorarà la capacitat per adaptar les formacions a la realitat i necessitats específiques de l'entitat contractant en el nivell avançat de formació.

Justificació del criteri:

L'orientació a l'entitat contractant i la formació a mida són aspectes que destaquen la importància de personalitzar les formacions per satisfer les necessitats específiques de l'organització. Aquesta adaptabilitat no només millora l'eficàcia de l'aprenentatge, sinó que també fomenta un major compromís dels empleats, ajudant a construir una cultura de seguretat robusta dins de l'entitat a partir de les bases de la seva pròpia estructura tècnica i organitzativa.

Criteris d'adjudicació quantificables mitjançant la mera aplicació de fórmules, fins a un màxim de 55 punts:

3. Entrenament actiu, fins a un màxim de 25 punts

3.1. Tasques d'entrenament als/a les usuaris/usuàries per comprovar que s'han adquirit i assimilat els conceptes relacionats amb la ciberseguretat, 10 punts:

Es valorarà que la formació inclogui activitats pràctiques que permetin als/a les usuaris/usuàries demostrar i reforçar els coneixements adquirits, mitjançant simulacions, exercicis pràctics, proves interactives o altres metodologies que permetin posar en pràctica els coneixements, que permetin acreditar que l'usuari ha adquirit els coneixements.

Justificació del criteri:

Les tasques d'entrenament són rellevants perquè serveixen per validar els coneixements adquirits per l'usuari. Les activitats pràctiques no només millora l'atenció de l'usuari a l'hora de fer l'aprenentatge, sinó que permet evidenciar els punts on cal millorar l'aprenentatge.

3.2. Informació correctora segons el resultat de les activitats, 10 punts:

Es valorarà el compromís d'incloure un retorn personalitzat de les pràctiques de l'usuari que ofereixin informació als usuaris de quins han estat els seus errors i quines són les respostes correctes.

Justificació del criteri:

La informació correctora permet a l'usuari visualitzar els seus errors i fixar la seva atenció en ells per tal de no repetir-los i augmentar així la seguretat del conjunt de l'organització.

3.3. Assignació automàtica de curs de formació, 5 punts:

Es valorarà el compromís d'incloure diferents cursos de formació, que s'assignaran a l'usuari de forma automàtica segons els seus coneixements.

Justificació del criteri:

La personalització dels cursos en funció de les necessitats de l'usuari no només millora l'eficiència i l'eficàcia del procés formatiu, sinó que també augmenta la motivació dels participants, facilita el seguiment del seu progrés i permet una ràpida adaptació a un entorn canviant en el camp de la ciberseguretat.

4. Presencialitat de la formació, fins a un màxim de 20 punts:

Es valorarà el compromís d'impartir les sessions de formació a les dependències de l'entitat contractant:

- 100 % presencial (a les dependències de l'entitat contractant), 20 punts.
- 50 % presencial, 15 punts.
- 25 % presencial, 10 punts.
- 100 % en línia, 0 punts.

Justificació del criteri:

La presencialitat de la formació ressalta la importància d'oferir sessions de formació a les dependències de l'entitat contractant. Aquesta opció no només facilita l'accés i la participació, sinó que també potencia la interacció, la captació de l'atenció de l'usuari, facilita el seguiment, la col·laboració i la personalització de l'aprenentatge, factors clau per al desenvolupament d'una cultura de ciberseguretat sòlida dins de l'organització.

5. Avaluació final dels cursos, 10 punts:

Es valorarà que les formacions continguin una prova final d'avaluació del curs.

Justificació del criteri:

L'avaluació final dels cursos no només mesura l'aprenentatge dels participants, sinó que també proporciona retroalimentació i informació sobre el seu aprofitament, incentiva la seva participació i valida la qualitat del curs, tot contribuint al millorament continu de la formació en ciberseguretat.

Lot 7 – Serveis de CSIRT:

Criteris d'adjudicació la quantificació dels quals depèn d'un judici de valor, fins a un màxim de 55 punts:

1. Procediment d'actuació, fins a un màxim de 35 punts:

Es valorarà el procediment d'actuació en cas d'incident i el de seguiment del servei, amb una explicació de la metodologia emprada, on s'especificaran tots els passos a seguir de cara al desenvolupament del servei, des de la fase de preparació, fins a la resolució de l'incident i l'entrega d'informes tècnics i executius posteriors a un incident.

Justificació del criteri:

Aquest criteri és fonamental per assegurar que l'empresa adjudicatària disposi d'un procediment clar i ben definit per a la gestió reactiva dels incidents de seguretat. Aquest anàlisi serveix com a indicador crític de la seva eficàcia i capacitat per respondre a incidents de manera oportuna i eficient. Una metodologia clara i ben definida, juntament amb un procés de seguiment que inclogui tots els passos a seguir, proporciona una base sòlida per a la gestió efectiva dels incidents de seguretat. Això contribueix a una mitigació àgil i eficient dels incidents.

2. Organització del servei i governança, fins a un màxim de 20 punts:

Es valorarà la millor idoneïtat de la proposta de l'estructura organitzativa del servei per part de l'empresa adjudicatària, l'equip de treball que desenvoluparà les funcions.

Justificació del criteri:

Aquest criteri és fonamental per assegurar que l'empresa adjudicatària disposi d'una estructura ben definida i eficient per gestionar els serveis de CSIRT. Una descripció detallada de l'equip de treball, la seva organització i el model de relació amb l'ens contractant millora la transparència, la responsabilitat i la comunicació, elements clau per a una gestió efectiva i coordinada dels incidents de seguretat, contribuint a minimitzar l'impacte sobre l'organització i millorant la seva resiliència davant de les amenaces cibernètiques.

Criteris d'adjudicació quantificables mitjançant la mera aplicació de fórmules, fins a un màxim de 45 punts:

3. Preu, fins a un màxim de 35 punts:

3.1. Tarifes de subscripció, fins a un màxim de 25 punts:

Es valorarà el preu de subscripció:

Nivell d'incidència	Tipus d'entitat	Valoració màxima
Nivell 1: Incidents lleus i moderats	< 15 treballadors	2,5
	15-50 treballadors	2,5
	50 -100 treballadors	2,5
	100 - 500 treballadors	2,5
	> 500 treballadors	2,5
Nivell 2: Incidents lleus, moderats i crítics	< 15 treballadors	2,5
	15-50 treballadors	2,5
	50 - 100 treballadors	2,5
	100 - 500 treballadors	2,5
	> 500 treballadors	2,5

Fórmula:

$$P_i = V_m * \left[\frac{P_{min}}{P_{of}}\right]$$

On:

- P_i = Puntuació de la proposta que es valora per cada tarifa.
- V_m = Valoració màxima de la tarifa.
- P_{min} = Preu de subscripció menor de les ofertes presentades per la tarifa que es valora.
- P_{of} = Preu de l'oferta per la tarifa que es valora.

La puntuació del criteri serà la suma de totes les puntuacions anteriors P_i:

$$P = \sum P_i$$

Justificació del criteri:

De conformitat amb el que estableix l'article 145.2 de la LCSP, els criteris qualitatius han d'anar acompanyats d'un criteri relacionat amb els costos, que, en aquest contracte, ha de ser el preu ("tarifes de subscripció" i "preu servei de consultoria post-incident i millora contínua"), atès que, donada la naturalesa del contracte, no és possible fer un plantejament basat en la seva rendibilitat, ni tampoc establir un criteri basat en el cost del seu cicle de vida.

Considerant que, amb caràcter general, tots termes del contracte s'han fixat i concretat en el PPT, es considera adequat assignar a les tarifes de subscripció la ponderació de 25 punts.

Justificació de la fórmula:

És una fórmula proporcional, atribueix la màxima puntuació a l'oferta més barata i no inclou llindars de sacietat.

No s'han determinat preus unitaris màxims, atesa la variabilitat de preus de les licitadores per la majoria d'aquests serveis.

3.2. Preu servei de consultoria post-incident i millora contínua, fins a un màxim de 10 punts:

Es valorarà el preu del servei de consultoria post-incident.

Fórmula:

$$P = V_m * \left[\frac{Plic - Pof}{Plic - Pmin}\right]$$

On:

P = Puntuació de la proposta que es valora.
V_m = Valoració màxima del criteri.
P_{lic}= Preu/hora màxim (200,00 €).
P_{min} = Preu/hora menor de les ofertes presentades.
P_{of} = Preu/hora de l'oferta que es valora.

Es tindran en compte dos decimals.

Justificació del criteri:

De conformitat amb el que estableix l'article 145.2 de la LCSP, els criteris qualitatius han d'anar acompanyats d'un criteri relacionat amb els costos, que, en aquest contracte, ha de ser el preu ("tarifes de subscripció" i "preu servei de consultoria post-incident i millora contínua"), atès que, donada la naturalesa del contracte, no és possible fer un plantejament basat en la seva rendibilitat, ni tampoc establir un criteri basat en el cost del seu cicle de vida.

Considerant que, amb caràcter general, tots termes del contracte s'han fixat i concretat en el Plec de Prescripcions Tècniques (PPT), es considera adequat assignar al preu servei de consultoria post-incident i millora contínua la ponderació de 5 punts.

Justificació de la fórmula:

És una fórmula proporcional que atribueix una puntuació superior a l'oferta més barata i menor a la més cara i guarda una proporció adequada en l'atribució a les ofertes intermèdies.

4. Presencialitat del servei, 10 punts:

Es valorarà el compromís de desplaçar l'equip a les dependències de l'entitat contractant si les circumstàncies o l'entitat així ho requereixen.

Justificació del criteri:

El criteri "Presencialitat del servei" es justifica per la importància de comptar amb un equip que pugui desplaçar-se a les dependències de l'entitat contractant quan les circumstàncies ho requereixin. La presència física de l'equip de seguretat en situacions crítiques permet una gestió més eficient i coordinada dels incidents, així com una comunicació immediata i directa amb els responsables de l'entitat. Aquest aspecte és especialment rellevant en casos d'incidents greus o complexos en què es requereix una resposta àgil i efectiva, ja que l'accés físic als sistemes i a la infraestructura facilita una intervenció més precisa i ràpida. A més, la presencialitat fomenta la confiança entre l'equip CSIRT i l'entitat, permet una millor comprensió del context i de les necessitats específiques de l'entitat i facilita la transferència de coneixement i bones pràctiques en seguretat, contribuint a un entorn de treball col·laboratiu i proactiu en la protecció dels sistemes.

Els criteris d'adjudicació estan suficientment especificats, atès que s'han fixat, de manera ponderada, amb concreció –els seus requisits, límits, modalitats i característiques, així com la seva vinculació necessària amb l'objecte del contracte–.

9. Paràmetres objectius que han de permetre identificar els casos en què una oferta es consideri anormal:

No s'estableixen paràmetres objectius que hagin de permetre identificar els casos en què una oferta en l'acord marc es consideri anormal.

10. Contribució a les despeses d'impuls, seguiment i coordinació de l'acord marc:

Entre els objectius del Consorci Localret hi ha dur a terme la contractació centralitzada de serveis de telecomunicacions i altres serveis en l'àmbit de les tecnologies de la informació i la comunicació (TIC), d'acord amb els principis de concurrència, neutralitat, transparència i no

discriminació mitjançant tècniques de racionalització de la contractació principalment." (art. 8.e dels Estatuts).

El Consell d'Administració de Localret, en sessió de 8 de novembre de 2022, va aprovar, formalment, la creació de la Central de Contractació del Consorci Localret com una unitat administrativa especialitzada dins de l'estructura organitzativa del Consorci, i va aprovar el seu Reglament d'organització i funcionament.

Pel que fa al règim econòmic de la Central de Contractació, el seu Reglament d'organització i funcionament preveu, expressament, que podrà establir-se un règim de contribució econòmica pels serveis de promoció, intermediació i gestió de les activitats de contractació centralitzada dels quals es beneficien les empreses licitadores i/o adjudicatàries dels contractes centralitzats.

En concret, la contribució pels serveis de promoció, intermediació i gestió de les activitats de contractació centralitzada s'ha determinat en base als criteris següents:

- El nombre de contractes basats en acord marc. La despesa que comporta a Localret la licitació d'un acord marc és directament proporcional al nombre de contractes basats del mateix. Tant la composició dels plecs de clàusules administratives particulars (PCAP) i de prescripcions tècniques (PPT) com la valoració d'ofertes és major com més gran sigui el nombre d'adjudicatàries i lots.

- L'oficina tècnica de seguiment dels contractes basats. La Central de Contractació posa a disposició de les entitats contractants i de les empreses licitadores l'assessorament dels tècnics de l'oficina tècnica de cada acord marc. Lògicament, a major nombre de contractes i més volum de productes o serveis, major dedicació és requerida dels tècnics de Localret.

- La tipologia d'objecte del contracte. També té un paper important els serveis o productes contractats i les seves modalitats de compra. Els canvis tecnològics o de modalitat de contractació que es puguin produir en la fase d'execució del contracte, requereixen de l'elaboració d'informes i procediments ad hoc que augmenten considerablement la dedicació del personal del Consorci.

A part del personal tècnic, que pot oferir assessorament i informar del funcionament i condicions de cadascun dels acords marc o contractes, es requereix del suport administratiu per al registre de comunicacions i processament de les mateixes.

El cost de licitació d'un acord marc és una despesa que no pot ser repercutida a les empreses adjudicatàries de manera inicial i directa al començament de cada contracte sinó que cal repercutir-la en el percentatge dels contractes basats juntament amb les despeses de l'oficina tècnica un cop les empreses han tingut un benefici econòmic.

Atès que no es pot conèixer ni garantir el nombre d'empreses adjudicatàries ni tampoc el volum dels contractes basats en número ni en import, cal fer una estimació global basada en contractacions anteriors.

Finalment, el valor resultant es confronta amb la seva adequació al mercat en base als valors del marge comercial de les empreses adjudicatàries. Igualment, es poden contemplar altres ajustos relacionats amb les característiques pròpies de la prestació que són singulars i es detallaran cas per cas. Aquests ajustos, tant el de mercat com els propis de la prestació, poden actuar en els dos sentits, bé, sigui incrementant el valor de la remuneració, o bé, disminuint-lo.

En definitiva, el valor de la contribució es fixa en proporció a la previsió de costos de l'acord marc, i tenint en compte la seva adequació al mercat i a les prestacions de cada licitació.

L'elaboració de plecs que regeixen aquest acord marc ha requerit una important dedicació, per ser un acord marc no treballat fins ara, per la diversitat de productes que ha d'incloure i per la disparitat de solucions que existeixen actualment en el mercat. Addicionalment, l'adquisició i fusió d'empreses del sector així com la variació en les modalitats de contractació ofereixen un moment de molta confusió per part dels compradors i això ha fet que haguem requerit un temps extra per tal d'elaborar els plecs.

La previsió és que el nombre de contractes arribi a 20 empreses en el lot 1, 10 empreses en els lots 2, 3, 5 i 6, i 5 empreses en els lots 4 i 7, esperant que en total es presentin més de 100 ofertes en el global de l'acord marc.

Respecte als contractes basats, es preveu que en el lot 1 siguin més nombrosos que en la resta de lots, però que no tinguin un import elevat i que siguin contractes amb repetició; en canvi, en la resta de lots (lot 2 a 7) es preveuen contractes d'import molt més elevat i de llarga durada, però amb més complexitat.

Es considera, addicionalment, que la venta de productes disposa d'un marge comercial inferior a la venta de serveis i per aquest motiu es redueix el percentatge de despesa del lot 1 i es manté el percentatge dels lots 2 a 7.

11. Clàusules i criteris socials i mediambientals:

De conformitat amb el que estableix l'article 1.3 de la LCSP, en tota la contractació pública s'han d'incorporar de manera transversal i preceptiva criteris socials i mediambientals sempre que tinguin relació amb l'objecte del contracte.

Els criteris socials i mediambientals es detallen en el PCAP.

12. Actuacions prèvies ja realitzades:

De conformitat amb el que es disposa en la Instrucció de 23 de desembre de 2021 de la Junta Consultiva de Contractació Pública de l'Estat sobre aspectes a incorporar en els expedients i en els plecs rectors dels contractes que es vagin a finançar amb fons procedents del Pla de Recuperació, Transformació I Resiliència, amb caràcter previ a la preparació del present expedient de contractació, i amb l'objectiu declarat d'assegurar que els principis aplicables al PRTR es compleixen adequadament en la present licitació s'han realitzat les següents actuacions prèvies:

12.1. Concepte de fita i objectiu, així com els criteris per al seu seguiment i acreditació del resultat:

Dins de les deu polítiques palanca que contempla el PRTR s'identifiquen trenta-un components, entre ells, el component 15. El Component 15, referit a "Connectivitat digital, impuls a la ciberseguretat i desplegament del 5 G", està orientat, pel que fa, específicament, a la ciberseguretat (I7), a "assolir l'impuls de la ciberseguretat, amb la finalitat d'enfortir les capacitats, incrementar el teixit empresarial i crear ocupació". L'objectiu específic d'aquest component 15.I7 és "estendre una cultura de ciberseguretat sostenible per als ciutadans i empreses, desenvolupar i enfortir la industria de ciberseguretat i identificar, transformar i desenvolupar el talent de ciberseguretat necessari".

En aquest context, i amb la finalitat de continuar impulsant la transformació digital a tot el territori nacional, recentment s'ha inclòs un nou eix a l'Agenda 2026 de l'Espanya Digital. Mitjançant aquest nou eix, es va crear el Programa de Xarxes Territorials d'Especialització Tecnològica (en endavant, "Programa RETECH"), que té per objectiu impulsar xarxes territorials d'especialització tecnològica a través de projectes regionals centrats en la

transformació i l'especialització digital. Aquest programa assegura la coordinació, col·laboració i complementarietat entre regions.

Per col·laborar en el Programa RETECH i, en particular, en els projectes relacionats amb la ciberseguretat, l'Institut Nacional de Ciberseguretat (en endavant, "INCIBE") s'hi ha adherit i, com a conseqüència, va llançar una invitació pública per establir aliances amb entitats, tant públiques com privades, amb l'objectiu de contribuir a la consecució del Component 15.I7 del PRTR i de l'Eix Estratègic 3 de l'Agenda 2026 de l'Espanya Digital.

En resposta a aquesta convocatòria pública, diverses Comunitats Autònomes, com Catalunya, la Comunitat Valenciana i Galícia, a través de diferents entitats –en el cas de Catalunya, l'Agència de Ciberseguretat de Catalunya, en el cas de Valencia, la Direcció General de Tecnologies de la Informació i les Comunicacions de la Conselleria d'Hisenda, Economia i Administració Pública de la Generalitat Valenciana, i en el cas de Galícia, l'Agència per a la Modernització Tecnològica de Galícia ("Amtega"), han presentat el projecte a gran escala denominat "Centre d'Innovació i Competència en Ciències de la Salut, Indústria Intel·ligent, Connectada i Excel·lència Operativa" (en endavant, "Projecte RETECH CCAA"). Aquest projecte, centrat en la ciberseguretat, s'alinea amb els objectius de l'Agenda 2026 de l'Espanya Digital i el PRTR.

Els objectius estratègics i operatius que es marca el PROJECTE CENTRE D'INNOVACIÓ I COMPETÈNCIA EN CIBERSEGURETAT són els següents:

<u>OE1: Cohesionar l'ecosistema de ciberseguretat nacional</u>:

- OP1.1. Identificar i mapar les activitats i capacitats dels integrants i fomentar activitats conjuntes i intercanvi d'informació entre els diferents agents. D'aquesta manera s'augmentarà la competitivitat, impulsant la cooperació i l'eficiència de recursos.
- OP 1.2. Promoure la col·laboració públic-privada per al desenvolupament de projectes de millora de la ciberseguretat en les diferents regions participants.
- OP 1.3. Fomentar l'estudi i recerca tecnològica mitjançant centres de col·laboració.
- OP 1.4. Implantar laboratoris de ciberseguretat sectorials que serveixin de camp de proves i entorn formatiu.

<u>OE2: Promoure el sorgiment i creixement de noves empreses en els quatre verticals d'interès de la ciberseguretat</u>:

- OP 2.1. Estimular la transferència de coneixement a noves empreses i StartUps amb el suport i la formació especialitzada (incubadores, acceleradors…).
- OP 2.2. Implantar laboratoris de ciberseguretat sectorials que serveixin de camp de proves i entorn formatiu.
- OP 2.3. Donar suport en diferents àmbits per al desenvolupament de l'activitat empresarial.
- OP 2.4. Implementar accions d'internacionalització en l'àmbit de la ciberseguretat.

<u>OE3. Fomentar la capacitació especialitzada en ciberseguretat</u>:

- OP 3.1. Fomentar de diferents programes de ciberseguretat, com CyberRange.
- OP 3.2. Generar plans de formació específics que ajudin a donar resposta a les necessitats formatives del personal especialista i laboral i, en conseqüència, retenir el talent.
- OP 3.3. Sensibilització i conscienciació de la ciutadania a través de diferents campanyes i mitjans.
- OP 3.4. Estimular l'adopció de solucions innovadores mitjançant showrooms i activitats de divulgació.
- OP 3.5. Elaborar guies pràctiques sobre ciberseguretat sectorials.

- OP 3.6. Crear coneixement, col·laborant amb les institucions acadèmiques i les pròpies companyies en la formació de personal altament capacitat, imprescindible per al canvi de model productiu i la transformació digital de l'economia.

OE4. Impulsar projectes innovadors, solucions i serveis avançats als reptes de ciberseguretat als quals s'enfronta la societat:

- OP 4.1. Analitzar potencials riscos i amenaces, ja siguin presents o futurs, així com de l'impacte de les diferents actuacions en els tres territoris.
- OP 4.2. Proporcionar propostes amb un valor diferencial, reduint els costos de la implementació de la ciberseguretat per a garantir l'èxit de les propostes.
- OP 4.3. Elaborar informes de tendències i prospectives en matèria de ciberseguretat.

Els sectors estratègics o pols específics sobre els quals versarà són: ciències de la salut, transport intel·ligent, indústria connectada i excel·lència operativa, amb la finalitat d'ampliar, desenvolupar i fomentar les capacitats tecnològiques i industrials cibernètiques necessàries per a garantir la seguretat digital en els sectors nomenats. En el Projecte es proposen a més cinc àmbits d'actuació transversals, els quals ajudaran a evolucionar els sectors comentats i treballar al voltant de l'àmbit formatiu i de desenvolupament de talent, d'innovació, potenciar la col·laboració públic-privada, desplegar solucions i serveis cibernètics i fomentar un espai de dades.

El Projecte RETECH CCAA va ser avaluat i aprovat per la Comissió d'Avaluació de l'INCIBE el 7 de desembre de 2022. Posteriorment, el 18 de desembre de 2023, INCIBE i les comunitats autònomes de Catalunya (a través de l'Agència de l'Agència de Ciberseguretat de Catalunya), la Comunitat Valenciana (a través de la Direcció General de Tecnologies de la Informació i les Comunicacions de la Conselleria d'Hisenda, Economia i Administració Pública de la Generalitat Valenciana) i Galícia (a través de l'Agència per a la Modernització Tecnològica de Galícia, AMTEGA) van formalitzar un conveni de col·laboració per a l'execució del projecte.
En virtut d'aquest acord, conegut com a "Acord RETECH", les comunitats autònomes participants es van comprometre a desenvolupar diferents accions i projectes, amb un model de finançament pactat en el qual:

- El 75 % del finançament prové d'INCIBE, amb càrrec als fons NextGenerationEU del Mecanisme de Recuperació i Resiliència (MRR).
- El 25 % restant prové de fons propis, privats o comunitaris

IV. En el cas de la Comunitat Autònoma de Catalunya l'Agència de Ciberseguretat és l'entitat responsable de la implementació del Projecte RETECH CCAA i de les actuacions derivades de l'Acord RETECH a Catalunya. Per tant, li correspon concretar els múltiples subprojectes i accions de ciberseguretat que promouran el desenvolupament tecnològic i incrementaran la confiança digital tant del govern autonòmic com dels ciutadans i empreses del territori Català. Pel que fa a la Línia d'actuació Ciberseguretat de Retech Excel·lència Operativa sobre entitats del món local, aquesta té la missió de millorar el seu estat de protecció en l'àmbit de la ciberseguretat.

El Consorci Localret podrà participar en l'execució del projecte RETECH CCAA; concretament, en la línia d'actuació Ciberseguretat de Retech Excel·lència operativa, en el marc d'un conveni de col·laboració a celebrar amb l'Agència de Ciberseguretat de Catalunya (ACC) (pendent de signatura en el moment de subscriure's aquest document).

12.2. Etiquetatge verd i etiquetatge digital:

De conformitat amb el que es disposa en l'Annex VI del Reglament (UE) 2021/241 pel qual s'estableix el Mecanisme de Recuperació i Resiliència, relatiu a la «Metodologia de seguiment per a l'acció pel clima», i en el qual s'estableixen les Dimensions i codis relatius als tipus

d'intervenció del Mecanisme, i el que es disposa en l'Annex I de la Guia per al disseny i desenvolupament d'actuacions concordes amb el principi de no causar un perjudici significatiu al medi ambient, elaborada pel Ministeri per a la Transició Ecològica i el Repte demogràfic, la Inversió 7 ("Ciberseguretat: enfortiment de les capacitats dels ciutadans, pimes i professionals, i impuls de l'ecosistema del sector") del Component 15 ("Connectivitat digital, impuls a la ciberseguretat i desplegament del 5G") del Pla de Recuperació, Transformació i Resiliència en la qual s'emmarca l'execució del contracte actual no tenen assignat un camp d'intervenció que contribueixi a objectius climàtics, per la qual cosa no tenen obligació de complir un condicionat específic referent a això.

En canvi, de conformitat amb el que es disposa en l'Annex VII del Reglament (UE) 2021/241 pel qual s'estableix el Mecanisme de Recuperació i Resiliència, relatiu a la «Metodologia per a l'etiquetatge digital en el marc del Mecanisme», i en el qual s'estableixen coeficients per al càlcul de l'ajuda a la transició digital de cada tipus d'intervenció, i el que es disposa en l'Annex I del document de treball dels serveis de la Comissió titulat "Anàlisi del pla de recuperació i resiliència d'Espanya" que acompanya al document Proposta de decisió de execució Del Consell per la qual es modifica la decisió d'execució del Consell (UE), de 13 de juliol de 2021, relativa a l'aprovació de l'avaluació del pla de recuperació i resiliència d'Espanya COM (2023) 576 final, les mesures d'execució de la inversió 7 del component 15 del PRTR tenen assignat un camp d'intervenció que contribueix a la transició digital amb un coeficient del 100 %.

			Clima		Digitalització	
Codi de la mesura/submesura	**Denominació de la mesura/submesura**	**Despeses estimades (milions EUR)**	**Àmbit intervenció**	**Coeficient %**	**Àmbit intervenció**	**Coeficient %**
C15.17	Cybersecurity: Strengthening the capacities of citizens, SME and professionals; Improving the sector's Cybersecurity ecosystem	524			054 quinquies	100%

De cara a respectar els coeficients establerta per la Comissió Europea a través de l'etiquetatge digital i, d'acord amb el camp d'intervenció 4 Administració electrònica, serveis públics digitals i ecosistemes digitals locals, dimensió 5 del DESI: serveis públics digitals, àmbit d'intervenció 011: «Solucions de TIC per a l'Administració, serveis electrònics, aplicacions», emmarcat en l'Annex VII del Reglament (UE) 2021/241 pel qual s'estableix el Mecanisme de Recuperació i Resiliència, el 100 % del pressupost del programa es destina a la transició digital.

12.3. Anàlisi de risc en relació amb possibles impactes negatius significatius en el medi ambient (DNSH), seguiment i verificació de resultat sobre l'avaluació inicial:

S'ha incorporat a l'expedient de contractació de l'acord marc actual un informe de compliment del principi DNSH en el marc d'execució del projecte RETECH CCAA, corresponent a la Inversió I7 del Component 15 del Pla de Recuperació, Transformació i Resiliència.

La principal conclusió que s'aconsegueix en aquest informe de compliment del principi DNSH, tal com s'arreplega literalment en aquest, és que les activitats a desenvolupar dins del projecte RETECH CCAA, no suposen perjudici al medi ambient sobre cap dels seus sis eixos d'actuació, de conformitat amb l'avaluació del principi DNSH que es troba continguda en el document del Component 15. I7 del PRTR.

12.4. Reforç de mecanismes per a la prevenció, detecció i correcció del frau, la corrupció i els conflictes d'interès:

En relació al reforç de mecanismes per a la prevenció, detecció i correcció del frau, la corrupció i els conflictes d'interessos, resulten d'aplicació obligatòria a aquest òrgan de contractació les mesures d'específiques incloses en el Pla antifrau de l'Ajuntament de Barcelona, que pot consultar-se en l'enllaç https//bcnroc.ajuntament.barcelona.cat/jspui/handle/11703/137612.

La participació en la licitació que es refereix el present plec suposa l'assumpció per part de les empreses licitadores i de les empreses adjudicatàries de l'acord marc de l'obligació de compliment de les mesures contingudes en el pla de mesures antifrau de l'òrgan de contractació, amb ple respecte a la normativa espanyola i europea en relació amb la prevenció, detecció i correcció del frau, la corrupció i els conflictes d'interessos i als pronunciaments que referent a la protecció dels interessos financers de la Unió Europea hagen realitzat o puguin realitzar les institucions de la Unió Europea. Són aplicable les definicions de frau, corrupció i conflicte d'interessos contingudes a la Directiva (UE) 2017/1371, sobre la lluita contra el frau que afecta els interessos financers de la Unió Europea (Directiva PIF), i en el Reglament (UE, Euratom) 2018/1046 del Parlament Europeu i del Consell, de 18 de juliol de 2018, sobre les normes financeres aplicables al pressupost general de la Unió (Reglament financer de la UE).

La presentació de proposicions suposa per part de les licitadores l'acceptació incondicional de l'obligació de respectar els principis d'igualtat, lliure concurrència, transparència i integritat durant la fase de licitació, comunicant immediatament a l'òrgan de contractació les possibles situacions de conflicte d'interessos, aparents o reals de les quals tingueren coneixement i que puguin afectar el procediment de contractació. Al seu torn, es comprometen a no realitzar accions que posen en risc l'interès públic, aplicant la màxima diligència en el compliment de la legalitat vigent.

Aquest expedient de contractació i la seva execució estarà subjecte als controls establerts per la Comissió Europea, l'Oficina de Lluita Antifrau (OLAF), el Tribunal de Comptes Europeu i la Fiscalia Europea, per a això es facilitarà a aquests òrgans l'accés a tota la informació requerida sobre el contracte.

Si és el cas, pel que fa als contractes basats finançats amb fons del PRTR, es podrà dur a terme una anàlisi de risc de conflicte d'interès amb caràcter previ a la valoració de les ofertes, en els termes definits en l'Ordre HFP/55/2023, de 24 de gener, relativa a l'anàlisi sistemàtica del risc de conflicte d'interès en els procediments que executen el Pla de Recuperació, Transformació i Resiliència. Per a això, tindrà accés a l'eina informàtica de data mining (MINERVA), amb seu en l'AEAT, en la qual incorporarà les dades que procedeixi per a la realització d'aquesta anàlisi.

En cas que per a un licitador no existeixin dades de titularitat real de l'empresa objecte de consulta en les bases de dades de l'AEAT, l'òrgan de contractació sol·licitarà aquestes dades al licitador. Aquesta informació haurà d'aportar-se a l'òrgan de contractació en el termini de 5 dies hàbils des que es formuli la sol·licitud d'informació. La falta de lliurament d'aquesta informació en el termini assenyalat serà motiu d'exclusió de la licitació.

A més de l'anterior, qualsevol persona que tingui coneixement de fets que pogueren ser constitutius de frau o irregularitat en relació amb el contracte actual, pugui posar aquests fets en coneixement de:

- El Servei Nacional de Coordinació Antifrau (SNCA), integrat en la Intervenció General de l'Administració de l'Estat (IGAE), per mitjans electrònics, a través del canal http://igae.pap.minhafp.gob.es/sitios/igae/es-es/snca/paginas/comunicacionsnca.aspx.

- L'Oficina Europea de Lluita contra el Frau (OLAF), quan les sospites de frau o corrupció afecten els interessos financers de la Unió Europea.

- És possible dirigir-se a l'OLAF per mitjà dels següents canals:

  - Per carta a: Comissió Europea, Oficina Europea de Lluita contra el Frau (OLAF), Investigacions i Operacions B-1049 Brussel·les, Bèlgica

- Per correu electrònic a: Olaf-courrier@ec.europa.eu
- Per mitjà de les línies de telèfon gratuït: http://ec.europa.eu/anti-fraud

- Oficina Antifrau de Catalunya. A fi d'atendre possibles denúncies relatives a la detecció d'un possible frau, o la seua sospita fundada, i les presumptes irregularitats, s'habilita l'adreça de correu electrònic analisi@antifrau.cat.

- Canal d'alertes de l'Agència de Ciberseguretat de Catalunya: https://ciberseguretat.bustiaetica.seu-e.cat/#/, específicament pel que fa als contractes basats en l'acord marc que siguin finançats amb fons del PRTR.

D'altra banda, és obligatòria l'emplenament de la Declaració d'Absència de Conflicte d'Interessos (DACI) per part de:

a) Titular o titulars de l'òrgan de contractació,
b) Participants en la redacció dels plecs del contracte.
c) Membres de les taules o juntes de contractació.
d) Membres del comitè d'experts o als tècnics que elaboren els informes de valoració en el si del contracte.
e) El contractista i tots els subcontractistes.

12.5. Compatibilitat del règim d'ajudes d'Estat i prevenció del doble finançament:

El règim d'ajudes d'Estat ve delimitat pels articles 107 a 109 del Tractat de Funcionament de la Unió Europea i en la seua normativa de desenvolupament. A més, La Comissió aclareix els elements clau relatius al concepte d'ajuda d'Estat en la Comunicació 2016/C 262/01 de la Comissió relativa al concepte d'ajuda estatal conforme al que es disposa en l'article 107, apartat 1, del TFUE. El Considerant 8 del Reglament (UE) 2021/241 del Parlament Europeu i del Consell, de 12 de febrer de 2021, pel qual s'estableix el Mecanisme de Recuperació i Resiliència, assenyala que les inversions privades també podrien incentivar-se a través de programes d'inversió pública, en particular, instruments financers, subvencions i altres instruments, sempre que es respecten les normes en matèria d'ajudes estatals. Addicionalment, i segons la referència per a gestors sobre ajudes d'Estat en el marc del PRTR inclosa en l'Annex II.D de l'Ordre HFP/1030/2021, de 29 de setembre, per la qual es configura el sistema de gestió del Pla de Recuperació, Transformació i Resiliència, no concorren tots els requisits per a trobar-nos davant una ajuda d'Estat:

1. ¿Estamos ante una ayuda de Estado conforme al art. 107.1 TFUE[1]? (Para serlo deben concurrir todos los requisitos siguientes). a) Que la ayuda sea otorgada por el Estado o por fondos estatales, bajo cualquier forma. Se entienden incluidas todas las Administraciones Públicas. b) Que la ayuda falsee o amenace con falsear la competencia. c) Que la ayuda favorezca a determinadas empresas o producciones. d) Que la ayuda afecte a los intercambios comerciales entre Estados miembro.	Sí	No.
Continúe únicamente en caso de haber marcado «SÍ».		

Respecte al doble finançament, el Reglament (UE, Euratom) 2018/1046, del Parlament Europeu i del Consell, de 18 de juliol de 2018, sobre les normes financeres aplicables al Pressupost General de la Unió (Reglament Financer), estableix expressament en el seu article 188 la prohibició del doble finançament com a principi general aplicable a les subvencions, assenyalant en l'article 191 que en cap cas podran ser finançats dues vegades pel pressupost les mateixes despeses. En el cas concret del Mecanisme de Recuperació i Resiliència, el considerant 62 del Reglament (UE) 2021/241, del Parlament Europeu i del Consell de 12 de febrer de 2021, estableix que les accions previstes en aquest Reglament han de ser coherents amb els programes de la Unió en curs i complementar-los, així com evitar el doble finançament procedent del Mecanisme i d'altres programes de la Unió de les mateixes despeses. Així mateix, l'article 9 del citat Reglament disposa que les reformes i els projectes d'inversió podran rebre ajuda d'altres programes i instruments de la Unió sempre que aquesta ajuda no cobreixi

el mateix cost.

En el present cas, si bé alguns contractes basats en l'acord marc podrien finançar-se amb fons del PRTR, no està previst que es puguin utilitzar fons d'altres instruments. A la finalització del contracte no resultarà necessari procedir a la revisió de finançament amb base als indicadors inclosos en l'Annex II.D de l'Ordre HFP/1030/2021, de 29 de setembre, per la qual es configura el sistema de gestió del Pla de Recuperació, Transformació i Resiliència:

1. ¿Está previsto que el proyecto financiado con fondos del Mecanismo de Recuperación y Resiliencia reciba también financiación de otros instrumentos, ya sean nacionales o europeos?	Sí	No
Continúe únicamente si se ha marcado «SÍ» en la pregunta 1.		
2. ¿Existe documentación acreditativa (por ejemplo facturas o certificaciones del órgano gestor) de que la financiación procedente de otros instrumentos no se ha empleado en cubrir los mismos costes financiados con fondos del Mecanismo de Recuperación y Resiliencia?	Sí	No
3. ¿Las actuaciones financiadas con fondos del Mecanismo de Recuperación Resiliencia y las financiadas con otros instrumentos han quedado reflejadas en el correspondiente sistema operativo de gestión (por ejemplo la Base de Datos Nacional de Subvenciones o la Plataforma de Contratación del Sector Público) o en otra base de datos con funciones de seguimiento y control (por ejemplo sistema ARACHNE)?	Sí	No
4. ¿El proyecto cuenta con su propio Código Único de Identificación de Proyecto, conforme a lo establecido en la Orden HAC XXX/2021, de XX de junio?	Sí	No
En caso de responder «NO» en cualquiera de las pregunta 2, 3 y 4, debería saltar la alarma.		

12.6. Identificació del perceptor final dels fons, sigui com a beneficiari de les ajudes, o adjudicatari d'un contracte o subcontractista:

Amb la finalitat de donar adequat compliment al mandat establert en la lletra d) de l'apartat 2 de l'article 22 del Reglament (UE) 2021/241 del Parlament Europeu i del Consell, de 12 de febrer de 2021, pel qual s'estableix el Mecanisme de Recuperació i Resiliència per a incorporar la informació específica relativa al perceptor final dels fons se seguirà el procediment indicat en l'article 8.2 de l'Ordre HFP/1030/2021, de 29 de setembre, en totes les actuacions que es realitzen en execució del contracte en el marc del Pla de Recuperació, Transformació i Resiliència.

Per a donar compliment al citat procediment, l'adjudicatari haurà d'emplenar una Declaració de cessió i tractament de dades en relació amb l'execució d'actuacions del Pla de Recuperació, Transformació i Resiliència, el model de la qual s'incorporarà al plec de clàusules administratives particulars.

12.7. Obligacions de comunicació.

De conformitat amb el que es disposa en l'article 9 de l'Ordre HFP/1030/2021, de 29 de setembre, en totes les actuacions que es realitzen en execució del contracte en el marc del Pla de Recuperació, Transformació i Resiliència, els contractistes i subcontractistes hauran d'exhibir de manera correcta i destacada l'emblema de la UE amb una declaració de finançament adequat que digui «Finançat per la Unió Europea – NextGenerationEU» juntament amb el logotip del PRTR. Quan l'emblema de la Unió Europea es mostri en associació amb un altre logotip (Localret, ACC), haurà de mostrar-se almenys de forma tan prominent i visible com els altres logotips.

L'emblema ha de romandre distint i separat i no pot modificar-se afegint altres marques visuals, marques o text. A part de l'emblema, no podrà utilitzar-se cap altra identitat visual o logotip per a destacar el suport de la UE.

Aquestes mesures d'informació i comunicació de les actuacions desenvolupades s'inclouran en cartells informatius, plaques, publicacions impreses i electròniques, material audiovisual, pàgines web, anuncis i insercions en premsa, certificats, etc.

Tots els cartells informatius i plaques hauran de col·locar-se en un lloc ben visible i d'accés al

públic.

12.8. Avaluació de risc de frau, corrupció o conflictes d'interès:

No s'adverteixen en el contracte actual un risc de frau, corrupció o potencials conflictes d'interès superiors o diferents dels que es puguin advertir altres licitacions del Consorci Localret. En conseqüència, es considera suficients les mesures de prevenció, detecció, correcció i persecució establides en el Pla antifrau de l'Ajuntament de Barcelona, al qual el Consorci Localret es va adherir, mitjançant acord del Consell d'Administració en sessió de 8 de novembre de 2022, que pot consultar-se en l'enllaç https//bcnroc.ajuntament.barcelona.cat/jspui/handle/11703/137612.

12.9. Finançament UE Next Generation Pla Recuperació, Transformació i Resiliència (PRTR):

Aquest acord marc s'emmarca, en part, en el projecte «RETECH CCAA» del programa RETECH (Programa de Xarxes Territorials d'Especialització Tecnològica) que forma part de la Inversió I7, «Ciberseguretat: enfortiment de les capacitats dels ciutadans, pimes i professionals; i impuls de l'ecosistema del sector», del component 15 del Pla de Recuperació, Transformació i Resiliència (Connectivitat digital, impuls a la ciberseguretat i desplegament del 5G), i són finançades amb fons del Mecanisme de Recuperació i Resiliència (MRR) de la Unió Europea, establert pel Reglament (UE) 2020/2094 del Consell, de 14 de desembre de 2020, pel qual s'estableix un Instrument de Recuperació de la Unió Europea per a donar suport a la recuperació després de la crisi de la COVID-19, i regulat segons Reglament (UE) 2021/241 del Parlament Europeu i del Consell de 12 de febrer de 2021 pel qual s'estableix el mecanisme de Recuperació i Resiliència.

Els contractes basats en aquest acord marc podran ser finançats en un 100 % per la Unió Europea – Next Generation EU amb càrrec al Mecanisme de Recuperació i Resiliència en execució del Pla de Recuperació, Transformació i Resiliència (PRTR).

Eva Guijarro
Cap de l'Àrea de Transformació Digital i Tecnologies

Joan Bosch
Cap de l'Àrea de Contractació