

1 Criteris d'adjudicació

CRITERIS OBJECTIUS (75 punts)

PROPOSTA ECONÒMICA (55 punts):

Es determinarà l'oferta econòmicament més avantatjosa, amb una puntuació màxima de 55 punts, i la resta puntuant-se de manera inversament proporcional, d'acord amb la següent fórmula:

$$P_v = \left[1 - \left(\frac{O_v - OM}{IL} \right) \times \left(\frac{1}{VP} \right) \right] \times P$$

P_v = Puntuació de l'oferta a Valorar

P = Punts criteri econòmic

OM = Oferta Millor

O_v = Oferta a Valorar

IL = Import de Licitació

VP = Valor de ponderació

Factor de modulació: 3

Justificació de l'assignació del valor 3 en el factor de modulació: Licitació en les quals s'ha d'exigir que la prestació s'executi amb un alt nivell qualitatiu, atesa la complexitat tècnica, i per ús posterior de serveis assistencials destinats directament a les persones. En un entorn canviant de manera continuada i on es requereix un alt nivell d'especialització, la qualitat del servei prestada és essencial per assegurar la protecció davant les ciberamenaces, per aquest motiu es desitja premiar un bon sistema i amb totes les funcionalitats possibles per sobre d'un estalvi econòmic.

Les ofertes presumptament anormals o desproporcionades s'apreciaran de conformitat amb el plec de clàusules administratives particulars.

Per a la resta de criteris objectius, s'aplicarà els següents criteris de valoració:

FortiPAM (5 punts)

La inclusió d'una solució de Gestió d'Accessos Privilegiats (PAM), amb els requeriments de llicenciament esmentats a l'apartat 1.3.1 de l'Annex 1 i integrada nativament amb l'arquitectura de seguretat perimetral es valora com un element crític per garantir la protecció de les credencials més sensibles de l'organització. Aquesta tecnologia permetria controlar, monitorar i auditar en temps real l'ús de comptes

d'administrador, mitigant dràsticament el risc de robatori d'identitat i els moviments laterals dins de la xarxa.

- Sí = 5 punts
- No = 0 punts

FortiDeceptor (5 punts)

Es valorarà la incorporació de tecnologies d'engany (Deception Technology), amb els requeriments de llicenciament esmentats a l'apartat 1.3.2 de l'Annex 1, dissenyades per a la detecció primerenca d'intrusions i amenaces avançades que hagin evadit els controls preventius tradicionals. Aquesta solució desplega esquers realistes dins de la infraestructura per atraure els atacants, permetent identificar activitats malicioses i moviments laterals en les seves fases inicials. La seva inclusió aporta una capa de seguretat proactiva que redueix significativament el temps de permanència (dwell time) de les amenaces a la xarxa i automatitza la resposta davant d'incidents sense generar falsos positius.

- Sí = 5 punts
- No = 0 punts

Trend Micro Security Expert (5 punts)

La valoració d'aquest servei respon a la millora que suposaria comptar amb un suport de nivell superior en ciberseguretat, garantint l'accés directe a enginyers i analistes especialitzats del fabricant davant d'incidències crítiques o dubtes de configuració complexa. Aquest servei asseguraria que l'organització disposés d'una capacitat d'anàlisi forense i consultoria tècnica avançada per optimitzar les polítiques de seguretat. La seva inclusió minimitzaria els temps de resolució davant de crisis i garantiria que la infraestructura de protecció es mantingués actualitzada enfront de vectors d'atac emergents, maximitzant així el retorn de la inversió tecnològica.

- Sí = 5 punts
- No = 0 punts

Trend Micro CREM (5 punts)

La inclusió de funcionalitats de Gestió de l'Exposició al Risc Cibernètic (CREM) per a tots els endpoints i servers es considera important per evolucionar d'una postura de seguretat reactiva a una de preventiva. Aquest mòdul permetria la identificació, avaluació i quantificació contínua de la superfície d'atac global de l'organització. Aquesta eina seria clau per optimitzar els recursos de l'equip tècnic, enfocant les accions de remediació i hardening en aquells actius que representen un major risc per a la seguretat de la institució.

- Sí = 5 punts
- No = 0 punts

CRITERIS SUBJECTIUS (25 punts)

Els criteris qualitatius han estat seleccionats d'acord a l'article 145.2 LCSP:

- ☒ Característiques funcionals i estètiques dels articles
- ☐ Accessibilitat
- ☐ Disseny per totes les persones usuàries
- ☐ Característiques socials
- ☐ Característiques mediambientals o innovadores
- ☐ Organització, qualificació i experiència del personal adscrit
- ☐ Comercialització i les seves condicions
- ☐ El servei posventa i l'assistència tècnica i els compromisos relatius a recanvis
- ☒ El procés de lliurament, el termini de lliurament o execució i seguretat del subministrament

Per a cadascun dels criteris de valoració qualitatius/tècnics avaluable de forma subjectiva, que a continuació es relacionen, es realitzaran les valoracions en els termes previstos en cadascun dels criteris, obtenint cadascuna de les ofertes, en cadascun dels criteris, la puntuació corresponent.

Posteriorment, en el cas que com a mínim una de les ofertes obtingui una puntuació igual o superior al 50% de la puntuació màxima establerta per a cada criteri, s'aplicarà a les puntuacions obtingudes inicialment de cada criteri la fórmula següent:

$$P_{op} = P \times \frac{VT_{op}}{VT_{mv}}$$

P_{op} = Puntuació de l'Oferta a Puntuar

P = Puntuació del criteri

VT_{op} = Valoració Tècnica de l'Oferta que es Puntua

VT_{mv} = Valoració Tècnica de l'oferta Millor Valorada

En cada criteri les puntuacions finals que es concediran a les empreses seran les que resultin d'aplicar aquesta fórmula.

No obstant, en el cas que cap de les ofertes obtingui una puntuació igual o superior al 50 % de la puntuació de cada criteri, no s'aplicarà la fórmula anterior.

Els criteris subjectius d'adjudicació són els següents:

Criteri	Valoració
Disseny General del servei	15

Gestió i planificació del projecte	5
Qualitat de la memòria tècnica	5

Els licitadors que no obtinguin una puntuació de 12 punts dins del l'apartat de criteris subjectius no passaran a la següent fase d'avaluació de l'oferta econòmica.

1.1.1 Disseny general del servei (15 punts)

Un servei de ciberseguretat es pot plantejar de moltes maneres diferents i cadascuna d'elles tindrà els seus punts forts i punts febles. És per això que valorar el plantejament global de disseny del servei és de vital importància, per tal de poder identificar aquells aspectes que cal treballar més profundament. En aquest sentit, dins del disseny general es valorarà en concret:

- **Metodologia de treball de l'OTSI i full de ruta ENS (5 punts)**

Es valorarà la qualitat i el detall de la metodologia proposada per a l'Oficina Tècnica de Seguretat (OTSI). En concret, es puntuarà positivament la presentació d'un pla de treball o full de ruta clar i realista per a l'acompanyament en la certificació de l'Esquema Nacional de Seguretat (ENS). Es tindrà en compte com el licitador planteja l'anàlisi de bretxes, la gestió documental, el suport davant l'auditoria i l'estratègia per involucrar els diferents departaments de l'organització en aquest procés.

- **Integració, Correlació i Visió Unificada mitjançant SIEM (5 punts)**

Atesa la diversitat de fonts d'informació (Fortinet i Trend Micro) i la inclusió d'un sistema SIEM, es valorarà la qualitat del disseny de l'arquitectura de monitoratge. En concret, es puntuarà la capacitat del licitador per definir casos d'ús de correlació que creuin la informació de xarxa i de l'endpoint, permetent detectar amenaces complexes que passarien desapercebudes analitzant cada element per separat.

- **Propostes de proactivitat vers el servei (5 punts)**

Un element clau per evitar amenaces de seguretat és la proactivitat, per això es valorarà la capacitat d'actuació de manera proactiva del servei d'operacions basant-se en les observacions i events recollits a les diferents eines. Es prendrà com a mesura per la valoració la quantitat d'hores dedicades diàries a aquesta revisió. Aquelles propostes que incorporin més hores d'anàlisi de les dades recollides i/o accions proposades resultat d'aquestes dades es valoraran més positivament.

1.1.2 Gestió i planificació del projecte (5 punts)

Un sistema de protecció de ciberseguretat és una solució complexa. És per això que es valorarà positivament aquells propostes que incorporin elements de gestió del servei per tal de preveure i comprovar la seva evolució al llarg del temps. També es valorarà en aquest apartat el projecte de desplegament dels nous elements, avaluant els terminis d'instal·lació, així com les mesures de prevenció de riscos que es prenguin per evitar talls de servei imprevistos.

1.1.3 Qualitat de la memòria tècnica presentada (5 punts)

En un projecte que demana una implementació el més ràpida possible, però que per altra banda exigeix la minimització d'errors, una bona memòria tècnica demostra tant un elevat coneixement de la solució, com l'entorn on s'ha d'implementar, i també una alta capacitat de gestió. Tots ells elements claus per a l'èxit d'aquest projecte.

Dins d'aquest apartat es valorarà la qualitat general de la memòria tècnica presentada, basant-se en aspectes com les accions contemplades en el pla de d'implantació, eines de gestió del projecte, anàlisi de riscos, etc