INFORME DE VALORACIÓ SUBJECTIVA: CONTRACTACIÓ D'UN SERVEI EXTERN DE CISO (CHIEF INFORMATION SECURITY OFFICER) PER A L'ENTITAT, AMB LA FINALITAT DE REFORÇAR EL SISTEMA DE GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ, GARANTIR EL COMPLIMENT DE LA NORMATIVA VIGENT EN MATÈRIA DE CIBERSEGURETAT I PROTECCIÓ DE DADES, I IMPULSAR EL DESENVOLUPAMENT, IMPLANTACIÓ I SUPERVISIÓ DEL PLA DE SEGURETAT DE LA INFORMACIÓ DE LA INSTITUCIÓ.

ANTECEDENTS

Els criteris subjectius o susceptibles de judici de valor de l'expedient CSCSI 6/2025, per a la contractació del servei extern de CISO (Chief Information Security Officer) per a l'entitat, amb la finalitat de reforçar el sistema de gestió de la seguretat de la informació, garantir el compliment de la normativa vigent en matèria de ciberseguretat i protecció de dades, i impulsar el desenvolupament, implantació i supervisió del Pla de Seguretat de la Informació de la institució.

EMPRESES SOTMESES A LA VALORACIÓ

Empreses
• **CYNEXIA CYBERSECURITY S.L.**
• **EVOLUTIO CLOUD ENABLER, S.A.U.**
• **FACTUM INFORMATION TECHNOLOGIES, S.L.**
• **OBJETIVO TARSYS SL**
• **SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U**
• **TUV RHEINLAND IBERICA ICT, S.A**

1. CRITERIS SUSCEPTIBLES DE JUDICI DE VALOR (SOBRE B): fins a 45 punts

a) *Enfocament del servei* (***20 punts)***

Aquest criteri té per objecte valorar la claredat, coherència i concreció de la proposta tècnica presentada pels licitadors, pel que fa a com entén i articulen el servei de CISO extern, dins el marc d'un contracte de 120 hores anuals.

Es busca un enfocament realista, mesurable i alineat amb les necessitats del CSC que permeti verificar la capacitació del licitador en la planificació, priorització i execució del servei amb un impacte tangible sobre la seguretat de la informació i el compliment normatiu.

Pel que la manera de avaluar aquest enfocament es basarà en els següents matisos.

Definició d'objectius i resultats esperats (10 punts sobre 20). Es valorarà:

- Existència d'una relació clara d'objectius específics adaptats al volum de dedicació (120h)
- Delimitació del que cobreix i què queda fora del servei. Tot i ser un servei basat en el preu/hora; és important que quedin delimitats aquells punts que es preveuen inclosos en el servei i aquells exclosos del mateix (si escau).
- Definició dels resultats esperats mesurables o verificables, com poden ser informe de diagnosi, revisió de riscos, protocol de resposta.
- Coherència entre els objectius i el temps disponible, les propostes desproporcionades o poc realistes reduiran la puntuació.

    - 0 punts.- Proposta genèrica, poc concreta, sense objectius.
    - 5 punts.- Proposta correcta: defineix objectius i abast, però amb poca concreció o sense límits o resultats mesurables.
    - 10 punts.- Proposta excel·lent: objectius clars, realistes, mesurables, adaptats a 120h, inclou què cobreix i què queda fora del servei.

Planificació temporal i estructuració del servei (10 punts sobre 20). Es valorarà:

- Existència d'un pla de treball o cronograma orientatiu amb distribució d'hores per fase o activitat.
- Definició d'un ordre lògic d'execució (diagnosi → proposta de millora → seguiment → informe final).
- Indicació de fites intermèdies o lliurables (ex: informe inicial, sessió de validació, tancament).
- Identificació de mecanismes de seguiment o control de l'execució (reunions, validacions, informes).

    - 0 punts.- No presenta cap planificació o és confusa.
    - 5 punts.- Planificació genèrica o incompleta. En referència als aspectes a valorar, doncs per exemple podríem tenir indicació de fites però no mecanismes de seguiment, en aquest cas la puntuació seria de 5 punts.
    - 10 punts.- Planificació estructurada, realista i verificable, amb dedicació coherent, fites planificades, seguiment o control de l'execució, etc.

b) Governança i coordinació ***(15 punts)***

Es valorarà de manera preferent la metodologia de treball proposada pel licitador, amb l'objectiu de determinar si el CISO extern pot integrar-se de forma efectiva en l'organització del CSC i donar resposta a les seves necessitats operatives, de seguiment i de coordinació amb les àrees de sistemes i protecció de dades.

Pel que fa a la manera d'avaluar aquest enfocament es basarà en els següents matisos.

- **Claredat i estructura de la metodologia de treball:** es valorarà al licitador que presenti un mètode de treball estructurat, amb fases definides, dinàmica de sessions, mecanismes de validació i eines concretes. En definitiva, la proposta ha de permetre entendre com s'organitzarà el servei en el dia a dia i com es gestionaran les tasques, demandes i imprevistos o urgències.
- **Capacitació d'adaptació a la realitat del CSC:** s'analitzarà si la proposta incorpora elements adaptats al context real del CSC (equip de sistemes reduït, necessitat de planificació eficient i coordinació fluida amb protecció de dades, entitat multicèntrica, i entramat empresarial complex). Les propostes genèriques o desconnectades del funcionament intern obtindran menor puntuació.
- **Definició de canals de comunicació i mecanismes de coordinació:** Es valorarà la claredat en la definició de reunions periòdiques, canals de comunicació, circuits de validació i formats de *reporting*. És important que el licitador entengui la necessitat de traçabilitat i governança.
- **Integració de bones pràctiques dins la proposta:** es valoraran les referències als marcs de seguretat ISO, ENS, NIST; i que les mateixes actuïn com eix vertebrador de la implementació.

    - 0 punts.- Descripció superficial, sense mètode, no adaptable a les necessitats diàries i específiques del CSC.
    - 5 punts.- Metodologia entenedora però genèrica. Referències teòriques sense aterrar.
    - 15 punts.- Metodologia clara, aplicada, amb fases i eines. Referències a ISO/ENS/NIST de manera pràctica i adaptada.

c) Millora de la seguretat de la informació ***(10 punts)***

Aquest criteri valora la qualitat i la solidesa tècnica de la proposta en relació amb com el licitador contribuirà a millorar la seguretat de la informació dins el marc de 120 hores. L'avaluació se centrarà en la metodologia específica aplicada a la gestió de riscos, vulnerabilitats, mesures de protecció i resposta davant incidents, i no en la planificació o la governança ja analitzades en altres criteris.

- **Capacitat per identificar i planificar riscos de manera operativa:** es valorarà la metodologia que pugui plantejar el licitador respecte detecció de riscos, vulnerabilitats o mancances, basat en l'evidència, revisió documental o eines de diagnosi. La proposta ha de mostrar com es prioritzaran els riscos per impacte i probabilitat evitant models teòrics genèrics. S'atorgarà més puntuació a aquell model que presenti un sistema de priorització realista i adaptat a l'escala del CSC.
- **Concreció de les mesures de millora proposables:** es valorarà que el licitador indiqui quin tipus de millores pot proposar dins les 120 hores (actualització de polítiques, protocols, controls, etc.) no entren en aquest punt l'execució de les mesures. Millores viables, aplicables i prioritzables i no dependents d'un desplegament extern.
- **Enfoc de la resposta davant incidents:** es valorarà la claredat amb la que es defineix com es donarà suport a la gestió i anàlisis d'incidents de seguretat. Es puntuaran millor les propostes que mostrin una aproximació pràctica, eficient i proporcionada, sense exigir recursos d'un SOC.

    - 0 punts.- Proposta superficial, teòrica o poc aplicable; no concreta millores ni metodologia.

- 5 punts.- Metodologia entenedora però genèrica; descriu marcs o models sense mostrar aplicació directa al CSC.
- 10 punts.- Metodologia clara, aplicada i específica; identifica riscos, proposa millores viables i defineix la resposta a incidents de manera pràctica i adaptada.

A. ENFOCAMENT DEL SERVEI (FINS A 20 PUNTS)

Aspectes a valorar	Puntuació màx.	Empresa	Puntuació atorgada	Justificació
Definició d'objectius i resultats esperats	Fins a 10 punts	CYNEXIA CYBERSECURITY S.L.	10	La proposta defineix de manera molt clara el rol del CISO extern, alineant-lo amb les funcions descrites al plec i evitant confusions amb serveis tècnics o d'auditoria. Els objectius del servei es formulen de manera concreta, amb una orientació clara a la governança de la seguretat, l'assessorament estratègic i la presa de decisions informades per part de la direcció. Es delimiten amb precisió els àmbits inclosos i exclosos del servei, fet especialment rellevant atès el límit de 100–120 hores anuals. Els resultats esperats es vinculen a evidències verificables (informes, seguiment d'indicadors, suport en incidents), demostrant una comprensió clara de les necessitats reals del CSC.
		EVOLUTIO CLOUD ENABLER, S.A.U.	8	La proposta defineix adequadament els objectius del servei de CISO extern, amb una cobertura clara dels àmbits de governança, gestió del risc, compliment normatiu i resposta a incidents. Els objectius són coherents amb el plec i amb la dedicació prevista, i es plantegen resultats alineats amb bones pràctiques del sector. No obstant això, l'enfocament reflecteix parcialment una lògica de gran proveïdor de serveis, amb una menor personalització del rol del CISO extern respecte a l'estructura concreta del CSC.
		FACTUM INFORMATION TECHNOLOGIES, S.L.	9	Factum defineix correctament l'abast del servei i els objectius principals del CISO extern, amb una delimitació clara de les exclusions. L'enfocament és coherent amb el plec, però amb una orientació menys marcada cap a resultats mesurables a nivell directiu. Els objectius es formulen de manera adequada, tot i que amb menor èmfasi en indicadors de seguiment i evidències recurrents, tot i haver-n'hi.
		OBJETIVO TARSYS SL	5	La proposta presenta els objectius del servei principalment enfocats al compliment normatiu i a l'anàlisi de riscos, especialment en relació amb l'ENS. Tot i que aquests aspectes formen part de les funcions del CISO extern, la proposta no desenvolupa de manera suficient el rol estratègic, transversal i continuat que descriu el plec. Els objectius es formulen de manera genèrica, amb escassa orientació a resultats mesurables, indicadors o evidències recurrents, fet que limita la capacitat de verificar l'assoliment efectiu del servei.
		SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U	7	La proposta presenta un enfocament clarament orientat al compliment normatiu, amb una definició més genèrica del rol del CISO extern. Els objectius es formulen de manera correcta, però amb menor orientació a resultats estratègics i de governança tal com estableix el plec.
		TUV RHEINLAND IBERICA ICT, S.A	5	La proposta defineix els objectius del servei principalment des d'una perspectiva de compliment normatiu, revisió i validació, pròpia d'un enfocament d'auditoria o tercera part independent. Tot i que es fa referència a funcions pròpies d'un CISO extern, aquestes no es desenvolupen com una funció continuada de lideratge i assessorament estratègic integrat en l'organització, tal com estableix el plec. Els objectius es formulen de manera correcta però genèrica, sense un desplegament clar de resultats operatius i evidències recurrents associades al dia a dia del CSC. Això limita la capacitat d'avaluar l'impacte real del servei dins el volum d'hores previst.

Aspectes a valorar	Puntuació màx.	Empresa	Puntuació atorgada	Justificació
Planificació temporal i estructuració del servei	Fins a 10 punts	CYNEXIA CYBERSECURITY S.L.	10	La planificació del servei està estructurada de manera coherent al llarg del període contractual, amb una seqüència lògica d'activitats que permet combinar tasques recurrents amb actuacions puntuals segons necessitats. La proposta facilita el seguiment de l'execució del servei i garanteix una utilització eficient del temps disponible. L'estructuració és realista i evita plantejaments excessivament ambiciosos que no serien assumibles dins el volum d'hores previst. El model presentat s'adapta bé a una prestació continuada del servei.
		EVOLUTIO CLOUD ENABLER, S.A.U.	8	Evolutio presenta una planificació clara, amb fases definides i una distribució ordenada de les activitats al llarg del període contractual. La proposta permet visualitzar l'evolució del servei i facilita el control de la dedicació temporal. Tot i això, la planificació està concebuda amb un cert nivell d'estandardització, fet que pot limitar lleugerament la flexibilitat d'adaptació a necessitats específiques puntuals del CSC.
		FACTUM INFORMATION TECHNOLOGIES, S.L.	9	La planificació del servei és coherent amb la dedicació prevista i planteja una seqüència lògica d'actuacions. La descripció de fases i fites és menys detallada, fet que pot dificultar el seguiment sistemàtic del servei al llarg del període contractual.
		OBJETIVO TARSYS SL	5	La planificació del servei és poc concreta i es limita a una descripció general d'activitats, sense una distribució clara de les hores, fases definides ni fites temporals identificables. No es visualitza com es garantirà una prestació equilibrada i continuada del servei al llarg del període contractual, ni com s'adaptarà a necessitats sobrevingudes. Aquesta manca d'estructuració temporal dificulta el seguiment i control del servei per part del CSC.
		SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U	7	La planificació del servei és existent però poc detallada pel que fa a fites, distribució de les hores i seguiment de l'execució. Això limita la visibilitat sobre com s'assegurarà una prestació continuada i equilibrada del servei.
		TUV RHEINLAND IBERICA ICT, S.A	6	La planificació es presenta mitjançant fases d'actuació àmplies, amb una orientació principalment seqüencial (anàlisi, revisió, recomanacions), però amb **poca concreció temporal** pel que fa a cadències, recurrència d'activitats i seguiment continuat. El model proposat s'adequa millor a intervencions puntuals o projectes tancats que no pas a una prestació continuada del servei de CISO extern. Aquesta manca de detall en la distribució de les hores i en l'estructuració del servei dificulta la visualització d'una integració real en el funcionament ordinari del CSC.

B. GOVERNANÇA I COORDINACIÓ (FINS A 15 PUNTS)

Aspectes a valorar	Puntuació màx.	Empresa	Puntuació atorgada	Justificació
Governança i coordinació	Fins a 15 punts	CYNEXIA CYBERSECURITY S.L.	15	Es fa referència a les normatives ISO i ENS de manera pràctica i adaptada. Cynexia presenta un model de governança complet i ben definit, amb una clara identificació de rols, canals de comunicació i mecanismes de coordinació amb les àrees de sistemes i protecció de dades del CSC. Es descriu la participació del CISO extern en espais de seguiment i presa de decisions, així com sistemes de reporting periòdic que permeten una supervisió efectiva del servei. La metodologia proposada és aplicable a la realitat organitzativa del CSC i facilita una integració fluida del servei sense generar càrregues innecessàries. Aquest enfocament garanteix una coordinació eficient i una visió transversal de la seguretat.
		EVOLUTIO CLOUD ENABLER, S.A.U.	13	Es fa referència a les normatives ISO i ENS de manera pràctica i adaptada. La metodologia inclou canals de comunicació, reunions periòdiques i mecanismes de reporting adequats, assegurant una supervisió correcta del servei. Tanmateix, el rol del CISO extern es presenta més com una figura de coordinació de serveis que com una integració orgànica dins l'estructura del CSC. Aquesta aproximació pot reduir lleugerament la proximitat i la capacitat d'adaptació a una organització amb recursos interns limitats.
		FACTUM INFORMATION TECHNOLOGIES, S.L.	12	Es fa referència a les normatives ISO i ENS de manera pràctica i adaptada. La proposta descriu mecanismes de coordinació amb el client, però pel que fa al model de governança, falta desenvolupar-lo en més detall. La definició de rols, comitès i cadències de seguiment és correcta però menys estructurada, reduint lleugerament la capacitat de supervisió continuada.
		OBJETIVO TARSYS SL	7	Es fa referència a les normatives ISO i ENS de manera pràctica i adaptada. La definició de la governança és limitada, amb una descripció poc detallada dels canals de comunicació, rols i mecanismes de coordinació amb les àrees clau del CSC. No s'identifica clarament la participació del CISO extern en espais de governança ni en processos de presa de decisions. L'enfocament és principalment tècnic i normatiu, amb una integració reduïda en l'organització i una capacitat limitada de coordinació transversal, aspecte clau segons el plec.
		SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U	13	Es fa referència a les normatives ISO i ENS de manera pràctica i adaptada. Sothis destaca positivament en la definició d'estructures formals de governança, amb comitès, periodicitat de reunions i mecanismes de seguiment clarament definits. Aquest enfocament facilita el control formal del servei, tot i que és més procedimental que estratègic.
		TUV RHEINLAND IBERICA ICT, S.A	6	Es fa referència a les ISO i ENS de manera pràctica i adaptada. La proposta descriu mecanismes de coordinació amb l'organització, però aquests es plantegen de manera general i formal, sense un desenvolupament suficient dels canals operatius, rols interns, freqüència de reunions ni mecanismes de seguiment adaptats a la realitat del CSC. El rol del CISO extern queda més vinculat a la supervisió i validació que no pas a la participació activa en espais de governança i presa de decisions. Aquesta aproximació limita la capacitat d'integració transversal amb les àrees de sistemes i protecció de dades, aspecte que el plec valora de manera significativa.

C) MILLORA DE LA SEGURETAT DE LA INFORMACIÓ (FINS A 10 PUNTS)

Aspectes a valorar	Puntuació màx.	Empresa	Puntuació atorgada	Justificació
Millora de la seguretat de la informació	Fins a 10 punts	CYNEXIA CYBERSECURITY S.L.	9	La proposta estableix una metodologia clara per identificar, prioritzar i gestionar riscos de seguretat, amb una aplicació pràctica de marcs reconeguts com ISO 27001, ENS i NIST. Les millores plantejades són concretes, realistes i alineades amb els objectius del contracte, evitant enfocaments teòrics o genèrics. Es contempla el suport en la gestió d'incidents de manera proporcionada, adaptada a l'escala i recursos del CSC. L'enfocament permet obtenir millores tangibles en la gestió de la seguretat de la informació.
		EVOLUTIO CLOUD ENABLER, S.A.U.	7	La proposta és sòlida des del punt de vista tècnic i metodològic, amb referències clares a marcs reconeguts i processos de gestió del risc i incidents. No obstant això, la concreció de les millores aplicables dins el límit d'hores del contracte és inferior a altres propostes més focalitzades, especialment pel que fa a la priorització operativa.
		FACTUM INFORMATION TECHNOLOGIES, S.L.	8	Les actuacions proposades són tècnicament sòlides i viables dins el volum d'hores previst, especialment en matèria de riscos i continuïtat. Es presenta doncs, una metodologia clara i aplicada, no obstant, la gestió pràctica d'incidents i la priorització d'accions podrien estar més desenvolupades.
		OBJETIVO TARSYS SL	6	Tot i ser una metodologia clara i aplicada, les propostes de millora es basen principalment en recomanacions derivades d'anàlisi de riscos i compliment normatiu, amb poca concreció en accions prioritzades i aplicables dins el volum d'hores previst. L'impacte potencial en la millora efectiva de la gestió de la seguretat de la informació és limitat, especialment en àmbits com la resposta a incidents, la governança operativa o la conscienciació de l'organització.
		SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U	6	La metodologia exposada és clara i les millores proposades són coherents i s'exposen de manera aplicada a la normativa internacional, però tenen un impacte limitat en termes de millora operativa tangible dins el volum d'hores previst. L'enfocament és correcte però poc orientat a accions prioritzades.
		TUV RHEINLAND IBERICA ICT, S.A	7	La proposta incorpora una metodologia clara amb referències sòlides a bones pràctiques i marcs reconeguts, aportant un enfocament metodològic correcte en matèria de seguretat de la informació. Tanmateix, les millores proposades es formulen majoritàriament com a recomanacions o resultats d'anàlisi, amb menor concreció en actuacions prioritzades i aplicables dins el límit de 100–120 hores. L'enfocament és adequat des d'un punt de vista conceptual, però menys orientat a obtenir millores tangibles i immediates en la gestió operativa de la seguretat.

2. RESUM DE LA PUNTUACIÓ TOTAL SUBJECTIVA DE JUDICI DE VALOR

- CYNEXIA CYBERSECURITY S.L.

Obté una puntuació de **44 punts**, del total de 45,00 punts.

- EVOLUTIO CLOUD ENABLER, S.A.U.

Obté una puntuació de **36 punts**, del total de 45,00 punts.

- FACTUM INFORMATION TECHNOLOGIES, S.L.

Obté una puntuació de **38 punts**, del total de 45,00 punts.

- OBJETIVO TARSYS SL

Obté una puntuació de **23 punts**, del total de 45,00 punts.

- SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U

Obté una puntuació de **33 punts**, del total de 45,00 punts.

- TUV RHEINLAND IBERICA ICT, S.A

Obté una puntuació de **24 punts**, del total de 45,00 punts.

La següent valoració queda representada en els quadres adjunts:

QUADRES DE VALORACIÓ FINAL DE VALORACIÓ SUBJECTIVA:

								PUNTUACIÓ OBTINGUDA DELS CRITERIS SUBJECTIUS	
		Punt. Màx.	CYNEXIA CYBERSECURITY S.L.	EVOLUTIO CLOUD ENABLER, S.A.U.	FACTUM INFORMATION TECHNOLOGIES, S.L.	OBJETIVO TARSYS SL	SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U	TUV RHEINLAND IBERICA ICT, S.A
A	Enfocament del servei	20	**20**	**16**	**18**	**10**	**14**	**11**
B	Governança i coordinació	15	**15**	**13**	**12**	**7**	**13**	**6**
C	Millora de la seguretat de la informació	10	**9**	**7**	**8**	**6**	**6**	**7**
TOTAL PUNTUACIÓ		45	**44**	**36**	**38**	**23**	**33**	**24**

3. PUNTUACIÓ FINAL

D'acord amb la valoració efectuada, l'empresa CYNEXIA CYBERSECURITY S.L. ha obtingut la màxima puntuació, de 44 punts sobre els 45 punts possibles, en els criteris de valoració subjectes a judici de valor.

Puntuació	**Empresa**
44	CYNEXIA CYBERSECURITY S.L.

Denisa Maria Crisan

Tècnica de l'Àrea de Protecció de Dades del CSC