INFORME D'AVALUACIÓ TÈCNICA DE LES PROPOSTES PER LA CONTRACTACIÓ DE SERVEI D'AVALUACIÓ DE L'EXPOSICIÓ DE L'AGÈNCIA EN L'ÀMBIT DE L'ATENCIÓ PRIMÀRIA I L'ÀMBIT DE LES ENTITATS PROVEÏDORES D'ATENCIÓ SOCIOSANITÀRIA I DE SALUT MENTAL DE LA GENERALITAT DE CATALUNYA – Lot 1

Expedient de contractació: CB25AMOPL5003
Data: 19 de Desembre de 2025
Tipus de contracte: Contracte de serveis.
Criteris d'adjudicació subjectius
Òrgan de contractació: Directora de l'Agència de Ciberseguretat de Catalunya.
Procediment: Procediment contractació basat.
Objecte: Servei de de suport per a la validació pràctica de les arquitectures de seguretat implementades durant el desenvolupament dels Sistemes TIC del projecte PADP, impulsat pel Servei Català de Salut a Catalunya.
Aquestes tasques de suport es focalitzen majorment en l'execució de proves tècniques realistes, que permetin avaluar l'efectivitat dels requeriments de seguretat, definits i implementats durant la fase de desenvolupament dels sistemes.

De conformitat amb RESOLUCIÓ per la qual es formalitza i s'articula el traspàs de l'execució del projecte "Pla d'atenció digital personalitzada" del Servei Català de la Salut a les entitats gestores: Institut de Diagnòstic per la Imatge, Agència de Ciberseguretat de Catalunya, Centre de Telecomunicacions i Tecnologies de la Informació i Fundació TIC Salut Social, en el marc de la mesura C11.I03 del Pla de Recuperació, Transformació i Resiliència - Finançat per la Unió Europea – NextGenerationEU, en col·laboració amb el Ministeri de Sanitat.

VALORACIÓ

Per tal de formalitzar el procediment de valoració, l'equip de treball ha identificat i analitzat els elements més rellevants de les ofertes requerides per donar compliment al Plec de prescripcions tècniques que regeix la licitació i, posteriorment, s'ha avaluat cadascun dels blocs d'acord amb els criteris de puntuació definits al Plec de clàusules administratives particulars.

En endavant, es farà referència a les empreses licitadores segons la següent taula:

Licitador	Referència
A2SEcure Tecnologias Informatica SL	A2Secure
ATECH ADVANCED SOLUTIONS SA	AYESA
S2 GRUPO DE INNOVACIÓN EN PROCESOS ORGANIZATIVOS, S.L.U	S2Grupo

Els criteris de valoració són els indicats en el Plec Administratiu i es detallen a continuació:

Criteri adjudicació	Puntuació

Solució tècnica proposada	**24**
Casos d'ús	**25**

a. SOLUCIÓ TÈCNICA PROPOSADA (fins a 24 punts)

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

Els conceptes sobre els que es farà la valoració són:

1. Processos per l'execució dels serveis, processos operatius de suport, i processos per a garantir la imparcialitat i objectivitat en les activitats. (fins a un màxim de 4 punts)

2. Planificació de les proves. Es valorarà la incorporació d'una planificació detallada que garanteixi la viabilitat de completar totes les avaluacions dins del termini requerit. (fins a un màxim de 4 punts)

3. Metodologia proposada per executar l'avaluació plantejada detallant les diferents kill-chains proposades i considerant diferent casuístiques que puguin esdevenir. (fins a un màxim de 8 punts)

4. Proposta per assegurar que l'avaluació manté com a referència les ciberamenaces més rellevants i les seves característiques. (fins a un màxim de 4 punts)

5. Equip de treball i estructura organitzativa per a l'execució del contracte, tenint en compte la dedicació, el perfil i el pla de treball. Es valorarà l'equip de treball dedicat a l'execució del contracte tenint en compte els requeriment mínims, condicions i paràmetres establerts en l'apartat 3.3 del Plec de prescripcions tècniques. (Fins a un màxim de 4 punts)

A2Secure

Subcriteri 1 - Processos per l'execució dels serveis, processos operatius de suport, i processos per a garantir la imparcialitat i objectivitat en les activitats

L'oferta d'A2Secure descriu de forma detallada i coherent els diferents processos, tant operatius de suport, com els propis d'execució dels serveis, els quals encaixen en l'objecte principal del basat. A la vegada, la proposta descriu de forma clara i epecífica els processos per a garantir la imparcialitat i objectivitat en les activitats associades als serveis descrits al propi basat, així com el cicle de vida de les missions objecte del present basat. Igualment la proposta determina processos d'automatitzaió i millora de l'eficiència de les proves i estandarització com a valor afegit a la proposta.

Subcriteri 2 - Planificació de les proves

La proposta de d'A2Secure inclou una planificació detallada de les diferents rondes i activitats a executar des de l'inici del servei. Es defineix de manera clara una estratègia general d'execució, un cronograma general que encaixa amb els objectius del basat, i l'estructura de les microplanificacions per cada ronda. A la vegada, l'oferta presenta el model de gestió de la capacitat, així com un conjunt de riscos globals per assolir l'objectius del basat, determinar iniciatives de mitigació.

Subcriteri 3 - Metodologia proposada per executar l'avaluació

L'oferta de A2Secure descriu de manera detallada i coherent les diferents fases de la seva metodologia basada en estàndards de referència com per exemple OWASP, OSSTMM i MITRE ATT&CK, entre d'altres. Tanmateix, presenta de forma correcte, encara que amb poc detall, la descripció dels processos de disseny de Kill-Chains, així com dels processos vinculats a la simulació d'amenaces. A la vegada, la proposta incorpora 3 propostes d'escenaris de missions, adaptats a la realitat de l'àmbit objecte del basat, que evidencien coneixement del context del mateix, si bé es troba a faltar més detall al respecte. Per últim, determina de forma clara els procediments d'execució de les tècniques, així com els processos associats a la gestió de les evidències obtingudes i comunicació dels resultats.

Subcriteri 4 - Ciberamenaces més rellevants com a referència

L'oferta de A2Secure descriu de manera coherent però a molt alt nivell un enfoc de prestació de serveis Threat-Centric"el qual es basa en l'enriquiment de les missions amb la contextualització de les mateixes en base a la informació subministrada primerament pels serveis d'IOP de la pròpia Agència, enriquits amb la informació dels serveis de Threat intel de la pròpia entitat. A la vegada, presenta de forma molt general les principals amenaces del sector objecte del present basat.

Subcriteri 5 - Equip de treball i estructura organitzativa

La proposta d'equip i l'estructura organitzativa determina de forma clara dos principals perfils incorporats en l'oferta presentada , si ve es troba a faltar més alineament i valor addicional respecte les especificacions del plec, així com l'estructura organitzativa de l'equip. A la vegada, l'oferta incorpora un dimensionament de l'equip que encaixa amb l'objecte del basat, si bé es troba a faltar mes detall al respecte. Per últim, l'oferta determina polítiques específiques gestió del coneixement i rotació de l'equip adequades.

Subcriteri	Puntuació
Processos per l'execució dels serveis, processos operatius de suport, i processos per a garantir la imparcialitat i objectivitat en les activitats	3,00
Planificació de les proves	3,00
Metodologia proposada per executar l'avaluació	6,00
Ciberamenaces més rellevants com a referència	2,00
Equip de treball i estructura organitzativa	1,00
TOTAL	**15,00**

AYESA

Subcriteri 1 - Processos per l'execució dels serveis, processos operatius de suport, i processos per a garantir la imparcialitat i objectivitat en les activitats

L'oferta d'AYESA presenta de manera detallada i coherent els diferents processos, tant operatius de suport, com els propis d'execució dels serveis, els quals encaixen en l'objecte principal del basat, si bé es troba a faltar detall addicional que permeti determinar el valor afegit per la banda de l'entitat en el desplegament dels processos inclosos. A la vegada, la proposta descriu de forma general i a alt nivell els processos per a garantir la imparcialitat i objectivitat en les activitats associades als serveis descrits al propi basat.

Subcriteri 2 - Planificació de les proves

La proposta de AYESA inclou una planificació per a l'execució de les diferents rondes, desglossada en diferents fases i indicant tasques a realitzar dins de cadascuna d'elles que encaixen amb gran part dels requeriments establerts en el basat aplicable, sense gaire detall addicional. No obstant això, la proposta final determina terminis del sistema de rondes que no encaixen amb els requeriments del plec i que posen en risc l'execució efectiva del serveis inclosos en el present basat.

Subcriteri 3 - Metodologia proposada per executar l'avaluació

L'oferta d'AYESA contempla un marc metodològic basat en el modelat d'amenaces i dissseny de kill-chains basat en el consum d'intel·ligència de la pròpia Agència, el mapeig amb MITRE ATT&CK, i la selecció de cadenes d'atac a cada sistema PADP, el qual encaixa en l'objecte principal del basat. A la vegada, l'oferta determina, a molt alt nivell i sense detall que permeti determinar valor addicional, les principals proves manual i automàtiques que es duran a terme. D'igual forma, presenta una proposta d'industrialització adequada però amb poc detall.

Subcriteri 4 - Ciberamenaces més rellevants com a referència

L'oferta d'AYESA es basa en una metodologia per assegurar l'alineament amb les ciberamenaces aplicables la qual es recolza directament amb la funció d'IOP de l'Agència, seguint els requeriments del basat, si bé no s'identifica valor addicional rellevant als mateixos. A la vegada, especifica a alt nivell i sense gaire detall mecanismes d'actualització continua, i expressa el seu alineament amb els indicadors de servei determinats al basat.

Subcriteri 5 - Equip de treball i estructura organitzativa

La proposta d'equip i l'estructura organitzativa presentada es considera adequada. La mateixa descriuen els perfils de manera bastant detallada aportant detalls d'habilitats addicionals i formació dels mateixos i, respecte els requeriments del basat incorpora un perfil de suport/PMO tècnica, per garantir la qualitat en la gestió de lliurables, plantilles.... A la vegada, també s'inclou un poll d'experts com a reserva tècnica, per donar cobertura en cas de qualsevol incidència de l'equip que pogués posar en risc l'assoliment dels objectius del basat. Per últim, es determina un pla de substitució/reposició ràpida adequat.

Subcriteri	Puntuació
Processos per l'execució dels serveis, processos operatius de suport, i processos per a garantir la imparcialitat i objectivitat en les activitats	2,00
Planificació de les proves	1,00
Metodologia proposada per executar l'avaluació	2,00
Ciberamenaces més rellevants com a referència	1,00
Equip de treball i estructura organitzativa	2,00
TOTAL	**8,00**

S2Grupo

Subcriteri 1 - Processos per l'execució dels serveis, processos operatius de suport, i processos per a garantir la imparcialitat i objectivitat en les activitats

L'oferta de S2Grupo descriu de forma molt detallada i coherent els diferents processos, tant operatius de suport, com els d'execució dels serveis, els quals encaixen en l'objecte principal del basat, presentant un model d'avaluacions descrit com avançat el qual presentar característiques addicionals a les estàndards. A la vegada, la proposta descriu de forma molt clara i amb molt detall els processos per a l'execució dels serveis dintre de l'apartat Metodologia d'Auditoria, determinant propostes addicionals de valor, com poden ser realització d'informes addicionals en cas de que es detectessin alertes o vulnerabilitats concretes, entre d'altres.

Subcriteri 2 - Planificació de les proves

La proposta de S2Grupo inclou una planificació adequada de les diferents rondes i activitats a executar des de l'inici del servei. Es defineix de manera clara i amb molt detall les diferents fases incloses en la prestació del servei. Així mateix, es presenta una planificació completa de la iniciativa estructurada en rondes , amb molt nivell de detall sobre les activitats previstes (Pla de proves). incorporant proves addicionals que aporten un valor afegit a la mateixa.

Subcriteri 3 - Metodologia proposada per executar l'avaluació

La proposta presentada per S2Grupo destaca per una metodologia sòlida, molt ben detallada i coherent amb el tipus de servei i marcs de referència . Addicionalment, planteja un enfocament basat en simular les accions de potencials atacants davant les principals amenaces, aportant

exemples específics de tècniques i eines a utilitzar durant les proves tècniques. Aquest enfoc es considera molt realista i clarament adaptat a l'abast del servei. No obstant, es troba a faltar alguna referència a la possibilitat d'adaptar aquesta metodologia i lliurables a requeriments o estàndards ja definits per l'Agència. A més, la proposta incorpora una descripció detallada de molts tipus de proves aplicables.

Subcriteri 4 - Ciberamenaces més rellevants com a referència

La proposta de S2Grupo destaca per la seva integració operativa del coneixement acumulat en projectes reals dins del sector, amb una aproximació exhaustiva i ben contextualitzada. Es concreta la connexió entre les principals amenaces aplicables i les proves tècniques amb la inclusió de les mateixes de forma transversal a tota l'oferta, amb ús de simulació de *kill chains*, comprovació de controls i anàlisi d'explotabilitat. En conjunt, es considera una proposta completa, si bé es troba a faltar més detall relatiu a l'alineament amb la intel·ligència de l'Agència.

Subcriteri 5 - Equip de treball i estructura organitzativa

La proposta d'equip i estructura organitzativa compleix amb els requeriments especificats al plec. La proposta es considera altament detallada, tant a nivell de perfils, els quals es descriuen de forma molt específica determinant els rol i activitats dintre del projecte, com en l'estructura organitzativa. Addicionalment, s'afegeixen capacitats que es consideren de valor respecte el plec. Per últim, l'oferta determina polítiques específiques gestió del coneixement i rotació de l'equip adequades.

Subcriteri	Puntuació
Processos per l'execució dels serveis, processos operatius de suport, i processos per a garantir la imparcialitat i objectivitat en les activitats	4,00
Planificació de les proves	4,00
Metodologia proposada per executar l'avaluació	6,00
Ciberamenaces més rellevants com a referència	2,00
Equip de treball i estructura organitzativa	4,00
TOTAL	**20,00**

Puntuació final de criteri

La puntuació final d'aquest primer criteri resulta:

Licitador	Puntuació
A2Secure	**15,00**
AYESA	**8,00**
S2Grupo	**20,00**

b. CASOS D'ÚS (fins a 25 punts)

El licitador haurà de resoldre els casos d'ús formulats, donant resposta a tots els extrems que es detallen a continuació.

Es requereix realitzar la validació de l'arquitectura de seguretat d'un sistema d'informació del PADP. El licitador haurà de descriure el procés punt a punt que s'haurà de seguir, incloent, entre d'altres: requeriments identificats, decisions a prendre, bloqueigs a enfrontar, tasques a executar, lliurables a generar i en termes general qualsevol aspecte que asseguri la completesa del procés sencer.

Es valorarà positivament la proposta d'exemples de lliurables segons la solució tècnica proposada, l'ús adequat de metodologies i principals marcs de treball i ús que es fa del concepte de la ciberamenaça per dissenyar l'exercici.

A2Secure

A2Secure presenta un plantejament excel·lent, plenament alineat amb l'objecte del contracte, mitjançant un cas d'ús específic i perfectament personalitzat per a la validació de les arquitectures de seguretat d'un sistema de telemonitorització IoMT. El desenvolupament és molt realista i descriu de manera completa els principals processos involucrats, identificant amb claredat tant les tasques a executar com els requeriments necessaris per dur-les a terme amb garanties. Pel que fa a la gestió de bloqueigs i incidències, la proposta destaca especialment en definir escenaris concrets i versemblants, com el bloqueig del sistema de login en entorns de preproducció o la baixa mèdica d'un membre clau de l'equip, per als quals es proposen conjunts d'accions excel·lents i plans d'actuació molt adequats per minimitzar l'impacte sobre la missió.

La proposta suggereix una metodologia molt adequada basada en quatre fases per a cada missió de validació, oferint un plantejament complet, coherent i sense mancances rellevants. L'enfocament metodològic es recolza en la referència a marcs de treball àmpliament reconeguts com OWASP, OSSTMM, CVSS 3.1 i MITRE ATT&CK, fet que reforça l'alineació amb les bones pràctiques del sector. En conjunt, la metodologia proposada permetria executar missions de validació satisfactòries, consistents i amb un alt valor afegit.

La proposta inclou un conjunt de lliurables molt complet i excel·lentment definit, amb un alt nivell de detall i l'aportació d'exemples gràfics per a cadascun d'ells. S'hi contemplen, entre d'altres, informes tècnics i executius, informes de seguiment, avisos primerencs i bitàcoles d'activitat, la qual cosa permet comunicar de manera clara, estructurada i efectiva tant l'evolució com els resultats de les missions. Aquest enfocament assegura una transmissió òptima del valor generat i facilita la presa de decisions per part dels diferents perfils implicats.

La proposta adopta un enfocament threat-centric molt adequat, suggerint l'emulació d'adversaris específics a partir de la integració d'intel·ligència d'amenaces pròpia de l'Agència i de la mateixa companyia. Aquest plantejament aporta realisme i rellevància a les proves tècniques, alineant-les amb escenaris d'atac plausibles. Tot i així, l'apartat podria millorar-se amb un major nivell de detall en la definició dels perfils d'adversari, les tècniques concretes a simular i la seva traçabilitat amb els escenaris de prova, mantenint una valoració global molt positiva.

La puntuació resulta:

Licitador	Puntuació
A2Secure	**23,25**

AYESA

AYESA presenta un enfocament excel·lent i molt alineat amb l'objecte del contracte, plantejant un cas d'ús específic basat en un sistema de monitorització i atenció digital de pacients crònics amb ús de dispositius IoMT. Demostra un coneixement profund dels entorns i sistemes propis de l'àmbit assistencial, així com de les seves particularitats en matèria de seguretat. S'identifiquen de manera molt detallada els requeriments de seguretat associats a la missió, les decisions clau que cal prendre durant la seva execució i els principals bloqueigs o dificultats previsibles. Així mateix, es realitza un desglossament clar i complet de les tasques a executar, aportant una visió molt sòlida i estructurada de l'abast de les proves tècniques proposades.

La proposta destaca per una metodologia molt sòlida, coherent i plenament adequada per a l'execució d'una missió de validació completa. L'enfocament cobreix de manera molt equilibrada totes les fases del procés, des de les etapes inicials d'anàlisi teòrica de l'arquitectura i dels controls de seguretat existents, fins a l'execució de les proves tècniques i la presentació estructurada dels resultats. A més, es fa una referència encertada i ben integrada a marcs de treball reconeguts com MITRE ATT&CK, NIST CSF i NIST SP 800-53, reforçant la maduresa i l'alineació de la metodologia proposada amb bones pràctiques del sector.

La proposta defineix un conjunt de lliurables adequat i suficient, que recull els principals productes necessaris per comunicar el valor generat durant la missió de validació de seguretat. Aquests lliurables permeten entendre correctament els resultats obtinguts i les conclusions principals de les proves realitzades. No obstant això, la descripció no arriba a un nivell de detall exhaustiu, ja que no s'hi inclouen exemples gràfics concrets ni una definició més aprofundida del contingut de cadascun dels lliurables, fet que limita parcialment la seva concreció.

La proposta incorpora l'ús de la ciberamenaça com a element de referència per orientar les proves tècniques, suggerint que aquestes es basin en les amenaces més rellevants identificades per IOP. Aquest enfocament resulta pertinent i alineat amb l'objectiu de realitzar proves realistes. Tanmateix, el nivell de detall és limitat, ja que no s'especifica amb prou profunditat com es tradueixen aquestes amenaces en escenaris concrets, tècniques o vectors d'atac, fet que fa que l'aportació en aquest apartat sigui suficient però millorable.

La puntuació resulta:

Licitador	Puntuació
AYESA	**20,75**

S2Grupo

S2GRUPO SOLUCIONES DE SEGURIDAD, S.L.U. presenta un enfocament excel·lent i plenament alineat amb l'objecte del contracte, proposant l'execució d'una anàlisi de seguretat en modalitat de caixa grisa. Es descriuen amb gran profunditat les accions tècniques a dur a terme, evidenciant un coneixement expert i una elevada capacitat per completar amb garanties les missions requerides. S'identifiquen de manera molt acurada els requeriments de seguretat associats a cadascuna de les fases de la missió, així com les principals decisions a prendre durant la seva execució, oferint una visió clara, estructurada i molt completa de les tasques a executar.

La proposta defineix una metodologia molt sòlida basada en cinc fases per a una missió de validació completa, que cobreix tant els serveis exposats a Internet com la infraestructura interna que dona suport al sistema d'informació. L'enfocament metodològic inclou, a més, tasques addicionals de revisió i validació, com ara la revisió de polítiques, que reforcen la qualitat i la profunditat de l'anàlisi. Així mateix, es referencien de manera encertada marcs de treball i metodologies àmpliament reconegudes, com OWASP, OSSTMM, les metodologies del SANS Institute i MITRE ATT&CK, aportant consistència i alineació amb les bones pràctiques del sector.

Per a cada fase de la missió es defineix un conjunt de lliurables molt adequat, que permet recollir i comunicar de manera clara els resultats obtinguts i el valor generat durant les diferents etapes del procés. Tot i això, la proposta no incorpora exemples gràfics específics dels lliurables ni aprofundeix de manera exhaustiva en el contingut detallat de cadascun d'ells, fet que limita parcialment el nivell de concreció, tot i mantenir una valoració globalment positiva.

La proposta fa un ús adequat i ben integrat de la ciberamenaça, dedicant una fase específica de cada missió a la incorporació de coneixement d'intel·ligència d'amenaces. Aquesta informació s'aprofita de manera transversal al llarg de totes les fases del projecte, permetent simular de forma realista el comportament d'un atacant. Tot i que l'enfocament és sòlid i aporta un valor clar a les proves tècniques, es podria millorar amb un major nivell de detall en la definició de les amenaces, escenaris i tècniques concretes a simular.

La puntuació resulta:

Licitador	Puntuació
S2Grupo	**23,25**

Puntuació final de criteri:

La puntuació final d'aquest segon criteri resulta:

Licitador	Puntuació
A2Secure	**23,25**
AYESA	**20,75**
S2Grupo	**23,25**

PUNTUACIONS AGREGADES

Licitador	Conceptes a valorar		
	Solució Tècnica	Casos d'ús	Total
A2Secure	15,00	23,25	**38,25**
AYESA	8,00	20,75	**28,75**
S2Grupo	20,00	23,25	**43,25**

PUNTUACIONS COMPARATIVES

De conformitat amb la Directriu 1/2020, d'aplicació de fórmules de valoració i puntuació de les proposicions econòmica i tècnica de la Direcció General de Contractació Pública de la Generalitat de Catalunya, així com el Plec de Clàusules Administratives Particulars de la present licitació, un cop establerts els valors numèrics per a cada criteri i subcriteri s'ha d'aplicar la fórmula comparativa que s'indica a continuació per tal d'obtenir la valoració final.

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

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

Doncs bé, de conformitat amb l'anterior la puntuació final és la següent:

LOT 1:

Licitador	Conceptes a valorar		
	Solució Tècnica	Casos d'ús	Total
A2Secure	19,00	25,00	**44,00**
AYESA	9,67	22,31	**31,98**
S2Grupo	24,00	25,00	**49,00**

L'Hospitalet de Llobregat, la data i l'hora del present informe –a tots els efectes– és la que consta en l'encapçalament del present document, amb independència de la data de la signatura electrònica inserida,

Agència de Ciberseguretat de Catalunya