PLEC DE PRESCRIPCIONS TÈCNIQUES DEL

SERVEI DE SUBSCRIPCIÓ I GESTIÓ D'UNA SOLUCIÓ DE DETECCIÓ i RESPOSTA DAVANT CIBERAMENACES PER A L'IAS

PROCEDIMENT OBERT

CONTR/2024/0000000154

1 OBJECTE I ABAST DE L'EXPEDIENT ADMINISTRATIU

1.1 OBJECTE

L'objecte de la licitació és la contractació d'un servei de detecció i resposta ampliat contra possibles ciberamenaces a la plataforma tecnològica de l'IAS.

1.2.TERMINI I IMPORT DE LICITACIÓ

El termini d'execució del contracte serà per una anualitat contractual. Es preveu una pròrroga d'un any.

L'import màxim de licitació serà de **100.092,00 €** (IVA no inclòs); PVP de l'iva (21%) **21.019,32 €.**

L'import dels serveis (conceptualitzat per hores) i els mòduls i conceptes relatius a les hores, consten desglossats a la Taula de Determinació del Preu en arxiu adjunt a aquest Plec de Prescripcions Tècniques.

2 CONDICIONS GENERALS

El present plec de prescripcions tècniques particulars és d'aplicació conjunta amb el plec de clàusules administratives. **De manera complementària i subsidiària, i en tant no s'oposi al present plec serà d'aplicació el contingut de l'oferta dels licitadors**.

3 ESPECIFICACIONS TÈCNIQUES DEL SERVEI

3.1 DESCRIPCIÓ DE LA SITUACIÓ ACTUAL

L'IAS disposa d'una infraestructura TIC dissenyada i dimensionada per donar resposta a les necessitats tecnològiques requerides per donar servei a l'organització. Aquesta infraestructura compren tant estacions de treball per als professionals, com equips de comunicacions de dades, servidors per als sistemes d'informació i tot els components TIC necessaris per al seu correcte funcionament. El parc d'estacions de treball està distribuït en els diferents centres de treball (en el Parc Hospitalari Martí i Julià de Salt i resta de centres de salut mental i atenció primària de l'IAS). Els diferents sistemes d'informació de l'IAS donen servei a través d'una plataforma virtualitzada de servidors que es troba ubicada físicament en el CPD de l'hospital.

Un dels aspectes crítics i fonamentals que cal preservar en aquesta infraestructura tecnològica, és el de la ciberseguretat. Actualment l'IAS disposa de seguretat perimetral proporcionada per una sèrie de tallafocs, i d'un programari antivirus clàssic (EPP, Endpoint Protection Platform) present en les estacions de treball i servidors.

Per tal de millorar la protecció davant ciberamenaces, l'IAS vol disposar d'una plataforma de seguretat de nova generació que protegeixi els actius TIC de l'organització i que incorpori les tecnologies més noves i avançades en l'àmbit de la ciberseguretat (EDR, MDR, UBA,...).

3.2 REQUERIMENTS MÍNIMS DEL SERVEI

3.2.1 Descripció del servei

El servei haurà de d'incloure la subscripció en modalitat anual d'una solució tecnològica de detecció i resposta ampliada davant de ciberamenaces per a tots els endpoint i servidors de l'IAS. El servei també haurà de contemplar una gestió 24x7 de l'operació de la plataforma.

3.2.2 Dimensionament del servei

El servei de la plataforma de seguretat ha d'estar dimensionat per donar cobertura com a mínim a un volum de:

- 1700 estacions de treball
- 200 servidors

3.2.3 Requeriments funcionals mínims del programari

El programari ha de proporcionar les següents funcionalitats:

3.2.3.1 Antivirus NextGen (NGAV)

Ha d'analitzar els arxius en repòs i els arxius no executables per a protegir-los contra codi maliciós conegut.

- Antivirus d'última generació per a la prevenció de malware.
- Protecció contra codi maliciós mitjançant anàlisi estàtic basat en intel·ligència artificial.
- Protecció contra l'explotació basada en el comportament.
- Protecció de macros i scripts contra els atacs sense arxius basada en el comportament.
- Identificar i prevenir l'execució de malware amb signatures conegudes

3.2.3.2 Endpoint Detection and Response EDR

- Detecció i resposta per prevenir, detectar i respondre a les amenaces a nivell més avançat tant conegudes com desconegudes en tot l'entorn.
- SSDEEP Scan: utilització d'un algorisme de compressió que busca similituds amb un codi maliciós (conegut com a Fuzzy fingerprints).
- Patrons de memòria: anàlisis de la memòria carregada d'un host a la recerca de processos per identificar patrons d'activitat, estructura i comportament de dades, dades amb cadenes sospitoses i similituds amb codi maliciós conegut, activitat de codi maliciós, processos de càrrega de DLLs sospitoses o malicioses a la memòria per obtenir accés a àrees sensibles del sistema operatiu o ser injectades en altres processos.
- Tecnologia de detecció avançada (ADT): eines heurístiques per a la inspecció de sistemes operatius a la recerca de comportaments nocius originats per codi maliciós i atacs amb o sense arxius. Això detecta activitats malicioses en processos legítims com PowerShell o cmd. ADT analitza l'estructura d'un comandament, els seus resultats i la connexió entre el comandament i el procés primari, buscant patrons maliciosos.

3.2.3.3 Network Detection and Response (NDR)

- Analitzar l'activitat per a detectar atacs a la xarxa, incloent:
    - Robatori de credencials basat en la xarxa (suplantació de ARP, responedor DNS)
    - Moviments laterals en la xarxa
    - Comunicació sortint maliciosa (C2C, suplantació d'identitat o phising)
    - Reconeixement basat en la xarxa (atacs d'escaneig)
    - Filtració de dades basada en la xarxa (tunelització a través de diversos protocols).

3.2.3.4 User Behavior Analytics (UBA)

- Capacitat d'aprendre el comportament d'usuaris i entitats per a detectar activitats inusuals i alertar sobre aquests comportaments sospitosos.
- Ha de poder utilitzar informació associada, com rol, grup, geolocalització, hores de treball i més per definir patrons de comportament normals, i després detectar automàticament activitats sospitoses, com inicis de sessió per primera vegada i fora d'hora.

3.2.3.5 Esquers (Deception)

- Funcionalitat d'esquer o "Deception" que permeti simular superfícies artificials de ciberatac basada en credencials i hosts fake (Honeypots). Possibilitat de crear:
    - Robatori de credencials amb contrasenyes parany
    - Moviment lateral amb connexions parany
    - Exfiltració de dades amb arxius de dades parany

3.2.3.6 Sandbox

- Haurà de proporcionar entorn de sandbox tant per a anàlisis estàtics d'arxius com per a anàlisis dinàmics de processos permetent una investigació segura dels elements sospitosos.

3.2.3.7 24x7 Threat Hunting

Capacitat per poder fer cerques actives d'amenaces de xarxa no descobertes.

- Disponibilitat 24/7.
- Exclusions, llistes blanques i túnels
- Anàlisi On Demand
- Instruccions de correcció
- Monitorització d'alertes
- Caça d'amenaces
- Investigacions d'atacs

3.2.3.8 Threat Intelligence

- Protecció de memòria en temps real: Detecció i bloqueig de les cadenes de memòria que estan associades amb el ransomware.
- Filtrat d'arxius en temps real: Detecció i evitar que les aplicacions no aprovades escriguin en diversos tipus d'arxius, impedint l'accés a actius importants de l'empresa.
- Filtrat de components crítics: protecció de contrasenyes del sistema operatiu perquè el ransomware no pugui recopilar credencials ni propagar-se per tota la xarxa.

3.2.3.9 Control de dispositius

- Detecció i bloqueig dels dispositius d'emmagatzematge externs que s'insereixen en el punt de connexió (per exemple, un dispositiu USB o una targeta SD).

- Creació de perfils de control de dispositius d'emmagatzematge: Cada perfil ha de assignar-se a un grup d'escaneig diferent i poder incloure normes com dispositiu de connexió autoritzat o no autoritzat segons l'ID del dispositiu o el tipus de dispositiu.

3.2.3.10 Gestió de vulnerabilitats

- Recol·lecció de les vulnerabilitats del host i de la informació avançada del sistema.
- Inventari d'actius: revisió i gestió dels actius connectats, els arxius, les configuracions i els certificats, així com adoptar mesures de protecció específiques per a cada actiu.

3.2.4 Requeriments mínims de prevenció i detecció

La solució ha d'identificar:

- Arxius maliciosos i evitar la seva execució, inclosos virus, trojans, ransomware, spyware, cryptominers, i qualsevol altre tipus de malware , utilitzant com a mínim les següents tecnologies:
    - Protecció per signatures
    - Anàlisis estàtics de Machine Learning
    - Anàlisis dinàmics amb Sandbox en temps real
    - Intel·ligència d'amenaces
    - Integració AMSI
- Comportament maliciós d'arxius executats, processos en execució, modificacions de registre, accés a la memòria i finalitzar-los en temps d'execució, o generar una alerta utilitzant com a mínim les següents tecnologies:
    - Supervisió de l'accés a memòria
    - Procés d'anàlisi de comportament (heurística)
    - Alta similitud (fuzzy hashing)
    - Intel·ligència d'amenaces
- Comportament maliciós del compte d'usuari, indicatiu de compromís previ, utilitzant com a mínim les següents tecnologies:
    - Configurar polítiques d'activitat d'usuari (infracció de política)
    - Línia base del perfil de compte d'usuari (detecció d'anomalies)
- Interacció maliciosa amb arxiu de dades, amb tecnologia d'esquers, generant fitxers "Decoy".
- Filtració de dades a través de protocols legítims (túnels DNS, túnels ICMP), utilitzant com a mínim les següents tecnologies:
    - Seguiment de trànsit de xarxa (NTA)
    - Seguiment d'accés a fitxers (File Access Monitoring)

La solució ha de suportar:

- Creació de regles per excloure rangs de IP/adreces específiques, bloquejant IPs malicioses i dominis.

La solució ha d'identificar, bloquejar i alertar:

- Atacs d'escalat de privilegis, utilitzant com a mínim la tecnologia de seguiment de processos.

- Atacs de reconeixement (escaneig), utilitzant com a mínim la tecnologia NTA.
- Intents de robatori de credencials des de la memòria (bolcat de credencials, força bruta) o trànsit de xarxa (suplantació d'identitat ARP, responedor DNS), utilitzant com a mínim les següents tecnologies:
    - Seguiment de memòria
    - Seguiment de comptes d'usuari
    - Seguiment de trànsit, comportament i resposta de xarxa (NDR)
    - Tecnologia d'esquers, generant fitxers "Decoy".
- Ús d'eines d'atac comuns (Metasploit, Cobalt, Empire, etc.) utilitzant com a mínim la tecnologia de seguiment de processos.
- Moviments laterals (SMB Relay, pass the hash, etc.) utilitzant com a mínim les següents tecnologies:
    - Seguiment de trànsit de xarxa (NTA)
    - Tecnologia d'esquers, generant usuaris "Decoy".
    - Tecnologia d'esquers, generant connexions de xarxa "Decoy".
    - Tecnologia d'esquers, generant equips "Decoy".

La solució ha de tenir:

- Mecanisme intern de protecció contra l'accés i manipulació d'usuaris no autoritzats. Alerta i bloqueig davant de qualsevol intent de manipulació o desactivació.
- Funcionalitat de creació de perfils de control de dispositius d'emmagatzematge que permetrà detectar i bloquejar els dispositius d'emmagatzematge extern que s'insereixen en el punt de connexió (per exemple dispositiu USV o targeta SD).
- La capacitat de detectar i bloquejar comunicacions a dominis maliciosos, utilitzant com a mínim la tecnologia d'anàlisis de dominis.
- La capacitat de crear esquers (Decoys, Honeypots) sense necessitat d'instal·lar cap servidor On Premise i gestionats per l'agent únic de tota la solució.

3.2.5 Requeriments mínims de resposta, investigació i reparació

La solució ha de suportar:

- Aïllament, mitigació de presència i activitat maliciosa, localment en el endpoint amb les següents capacitats mínimes:
    - Executar comanda coordinada (com interfície CMD)
    - Obrir un Shell remot
    - Executar scripts o arxius des d'una ubicació de xarxa o mapejar una unitat
    - Tancar un endpoint i/o servidor
    - Aïllament d'un endpoint/servidor de la xarxa
    - Eliminació d'un arxiu (inclosos els arxius d'execució actius)
    - Posar un arxiu en quarantena
    - Matar un procés
    - Eliminació d'un servei i/o tasca programada

    - Bloqueig d'un usuari local o d'un usuari de domini
    - Reset de contrasenya d'usuari
    - Bloqueig de comunicacions en funció del destí
    - Desconnexió de targetes de xarxa
    - Canvi d'adreça IP
    - Capacitat d'editar un arxiu HOST
- Aïllament i mitigació de presència i activitat maliciosa a nivell mundial en tot l'entorn amb les següents capacitats mínimes:
    - Deshabilitar usuari
    - Reset de contrasenya
    - Bloquejar IP
    - Bloquejar domini
    - Bloquejar port
- Respostes automatitzades:
    - Playbooks de resposta preestablerts que es proporcionin llestos per a ser utilitzats
    - Playbooks de resposta personalitzats creats per l'administrador
    - Rollback

La solució ha de mostrar:

- La cadena d'events, objectes relacionats resultants d'un incident amb una visualització gràfica de l'incident mostrant:
    - Events
    - Dades relacionades sobre la víctima
    - Dades relacionades sobre l'agressor
    - Dades relacionades sobre la relació dels artefactes
    - Dades amb tot l'arbre de processos
    - Cadena d'events

La solució ha d'incloure:

- Motor d'investigació automàtic sobre els events de seguretat detectats que:
    - Permeti detectar qualsevol persistència
    - Mostrar la causa arrel
    - Mostrar els elements compromesos
- Capacitat de remeiar, sempre de manera autònoma, tot el que s'hagi identificat, eliminant de manera automatitzada els elements maliciosos identificats durant la fase d'investigació.

La solució ha de recopilar contínuament dades sobre totes les entitats i les seves activitats dins l'entorn permetent:

- Interacció amb arxius (crear, obrir, canviar nom, esborrar, executar)
- Execució de processos
- Inici de sessió d'usuari

- Trànsit de xarxa
- Canvis en el registre
- Programari instal·lat

La solució ha d'admetre:

- La visualització de dades d'entitat i activitat:
    - Cerca basada en patrons de comportament en tots els camps de cobertura (usuaris, arxius, màquines..)
    - Determinació de les regles i/o creació d'alertes i/o determinació del nivell de risc, en base a una resposta del patró de cerca i en temps real.
    - Habilitació de nombre d'usuaris per a realitzar activitats en paral·lel, en base als permisos d'usuari, i sense necessitat de desconnexió d'altre usuari per a l'execució de l'activitat.
- L'anàlisi dinàmic (sandbox)

3.2.6 Requeriments mínims de monitorització i control

La solució ha de suportar:

- File Integrity Monitoring (FIM) que asseguri la política en entorns fixes per alertar sobre qualsevol canvi en un arxiu.
- El descobriment desatès de diferents tècniques d'atac, cercant arxius, processos, connexions de xarxa i comptes d'usuari susceptibles de risc amb contrasenyes antigues.

La solució ha de proporcionar:

- Els mitjans per dur a terme la gestió d'inventari, permetent mapejar i correlacionar tots els actius dins de l'entorn, com endpoints, servidors, aplicacions instal·lades, comptes d'usuari i informes generats periòdicament.
- Recopilació i retenció de registres d'activitat i autenticació permetent la conservació durant el període de temps que exigeixen les distintes normatives.

La solució ha d'incloure:

- 24x7 Cerca Proactiva d'amenaces global (Threat Hunting).
- 24x7 Cerca Proactiva d'amenaces en Deepweb (Deep Hunting)
- 24x7 Cerca Proactiva d'amenaces en Darkweb (Dark Hunting)

La solució ha de tenir:

- Avaluació de vulnerabilitats integrada en el mateix agent, que descobreixi les actualitzacions de seguretat que falten en els sistemes i aplicacions. Els requeriments mínims són:
    - Revisió automatitzada de pegats de Windows
    - Control d'aplicacions instal·lades no desitjades
    - Control de versió mínima permesa d'aplicacions de tercers
    - Validació d'operativitat constant d'agents de tercers

3.2.7 Requeriments mínims d'infraestructura

La solució ha de tenir:

- Agent únic per a totes les tecnologies incloses (EPP, EDR, NDR, UBA, Deception...)
- Protecció amb contrasenya per a la desinstal·lació de l'agent únic
- Protecció total contra la finalització del servei
- Mínim impacte de l'agent en el rendiment de l'endpoint i/o servidor amb:
    - Possibilitat de limitar l'ús de CPU fins a un consum màxim del 5%
    - Consum mig de RAM màxim de 100 MB a cada endpoint i/o servidor.
- Opcions flexibles d'implementació per a la consola de gestió per adaptar-se a diversos tipus d'entorns (On Prem, SaaS, Híbrid)
- Instal·lació ràpida en tots els endpoints i servidors
- Instal·lació sense necessitat de desinstal·lació de l'anterior antivirus
- Comunicació xifrada entre el servidor d'administració i els agents.
- Coexistència amb tot el programari comercial instal·lat en endpoints i servidors.
- Coexistència amb tots els antivirus del mercat que puguin estar instal·lats en els endopoints i servidors.
- Coexistència entre endpoints, arxius, processos, activitat de l'usuari i trànsit de xarxa de forma totalment autosuficient, eliminant la necessitat de configuració manual de regles o polítiques.

El programari de la plataforma de seguretat haurà de poder instal·lar-se en les següents versions de sistemes operatius com a mínim:

- Sistemes Windows:
    - Sistemes operatius d'estacions de treball: Windows XP Service Pack 3 y superior, Windows Vista Service Pack 1 y superior, Windows 7 Service Pack 1 y superior, Windows 8,Windows 8.1, Windows 10, Windows 11.
    - Sistemes operatius de servidors: Windows Server 2003 Service Pack 2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022.
- Sistemes Linux:
    - Ubuntu 16.04 i superior, RedHat 7 y superior, Centos 6.9 y superior, Fedora 23 i superior, Debian 9.X i superior, Suse 12 i superior.
- Mac OS:
    - 10.13 ó superior.

3.2.8 Requeriments mínims d'operació del servei

La solució ha de tenir la capacitat de:

- Especificar la llista de regles d'exclusió d'alertes per als objectes seleccionats.
- Exportar la configuració actual del programa.

- Habilitar i deshabilitar certs tipus de notificacions.
- Qualificar la gravetat de les alertes de seguretat.
- Bloquejar l'accés a la configuració del programa per als usuaris finals.
- Especificar un programa per a descarregar actualitzacions, inclosa la capacitat de desactivar l'actualització automàtica.
- Implementació en múltiples sites que reportin a una única consola d'administració.
- Integració amb infraestructura de correu electrònic per a notificar al personal de seguretat en cas d'alertes.
- Integració amb productes SIEM comuns (a través de syslogs, API i a través de json).
- Informes estandarditzats i personalitzables.
- Recopilació i processament centralitzat d'alertes en temps real.
- Distribució centralitzada d'actualitzacions sense necessitat d'intervenció de l'usuari i de reiniciar l'endpoint i servidor.
- Extensió del període de retenció de dades predeterminat per equilibrar les polítiques corporatives i de privacitat.
- Opció d'ingerir syslogs de tercers procedents de qualsevol font i centralitzar-los tots en un sol panell.

3.2.9 Requeriments mínims del servei gestionat (MDR)

La proposta de servei ha d'incloure tant el programari que contempli tota la funcionalitat i operativa detallada en els punts anteriors, com un servei gestionat de detecció i resposta que proporcionarà l'adjudicatari. Aquest servei, en la modalitat de SOC, haurà de tenir els següents requeriments:

- Servei gestionat de detecció i resposta 24x7.
- Gestió d'events, alertes, consultes del client, i incidents.
- Anàlisis d'alertes i correlacions amb altres events que hagin pogut activar una alerta.
- Contacte proactiu davant de la detecció de determinades alertes o events, indicant quines accions específiques cal dur a terme per a resoldre l'incident.
- Capacitat per poder enviar des del client arxius sospitosos, per tal que es faci un anàlisis i es rebin indicacions de com procedir.
- Rebre conclusions sobre atacs investigats pel SOC.
- Suport en la implementació de IOC.
- Informes de detecció d'amenaces del SOC.
- Butlletins periòdics on s'informi dels avenços en matèria de ciberseguretat i de les actualitzacions crítiques a implementar.

3.2.10 Requeriments mínims d'instal·lació i implantació

El servei haurà de contemplar la implantació integral que inclogui la instal·lació, desplegament i parametrització de la solució en tots els actius, així com el seu seguiment i resolució de qualsevol incident que es pugui originar durant aquest procés.

El procediment necessari per a la implantació de la nova solució, haurà d'assegurar en tot moment el sistema des del punt de vista de la protecció i de la integritat de les dades, evitant interrupcions en els serveis, sempre que sigui possible. És a dir, s'ha de minimitzar el temps que un equip roman sense

protecció. Això implica que no es pot fer primer la desinstal·lació del producte actual de tots els equips i després la instal·lació del nou, sinó que cal plantejar un període de convivència de les dues solucions.

S'haurà de realitzar el desplegament de les polítiques necessàries, basades en les "best practices" del fabricant i en la operativa funcional interna de l'IAS, tant a nivell de servidor com d'equip personal. A l'IAS hi ha molts perfils d'equipaments singulars (estacions de treball, ordinadors, portàtils, servidors, equips d'electromedicina...) que requeriran polítiques especials i afinades.

Durant un període no inferior a quinze dies, des de la instal·lació de l'últim agent, caldrà donar suport immediat (sense necessitat d'obrir tiquets o incidències) a la resolució de possibles problemes que apareguin, relacionats amb el fet d'haver instal·lat un nou producte i unes noves polítiques de seguretat. És a dir, caldrà que el licitador configuri les excepcions necessàries que es detectin durant aquest període, per tal que els equips personals i servidors funcionin de la mateixa manera que ho feien abans de la instal·lació del nou agent. Es posarà especial èmfasi en la resolució de problemes relacionats amb el rendiment dels equips.

3.2.11 Requeriments mínims de formació

Amb l'objectiu de capacitar al personal TIC de l'IAS, el servei haurà d'incloure la formació necessària per tal de poder administrar i operar el programari licitat. El format del curs podrà ser en format virtual.

Amb la formació serà necessari proporcionar a l'equip TIC de tota la documentació necessària d'instal·lació, administració, operació i monitorització de la plataforma.

4 EXECUCIÓ DEL PROJECTE

El servei licitat ha de començar a estar operatiu durant la primera quinzena de Gener de 2025. Per aquest motiu és imprescindible que el desplegament de la solució es faci durant el mes de Desembre de 2024.

5 DOCUMENTACIÓ A APORTAR PEL LICITADOR: OFERTA ECONÒMICA (SOBRE C)

El licitador haurà de realitzar l'oferta econòmica tot complimentat **l'ANNEX 2 del PCAP**, amb el detall que s'indica a continuació:

5.1 OFERTA ECONÒMICA

Any 2025

Tipus endpoint	Nombre de llicències	Preu/any llicència (sense IVA)	Preu/any llicència (amb IVA)	Import Total (sense IVA)	Import Total (sense IVA)
Servidors	200				
Estacions de treball	1700				

5.2 MEMÒRIA DE REFERÈNCIES

S'inclourà Memòria on acrediti, en el seu cas, **les referències demanades en els criteris de valoració objectius (epígraf 7.2.2 d'aquest Plec).**

6 DOCUMENTACIÓ A APORTAR PEL LICITADOR: OFERTA TÈCNICA (SOBRE B)

L'oferta tècnica del licitador consistirà en l'aportació d'una memòria per tal d'acreditar cadascun dels apartats descrits en el punt d'especificacions tècniques del servei, segons es detalla seguidament:

- A/Descripció funcional i tècnica dels serveis de detecció i resposta davant ciberamenaces. El licitador elaborarà una **Memòria de la descripció funcional i tècnica de l'abast del contracte (epígraf 3 d'aquest Plec).** El licitador lliurarà l'oferta amb una estructura que s'adeqüi als punts exposats anteriorment, tot aportant la informació que cregui adient en cada un d'ells, de manera que permeti la seva avaluació de forma clara, evitant possibles interpretacions subjectives de la solució a aportar en cada un dels punts exposats.

Per tal que aquesta Unitat Tècnica de l'IAS pugui valorar ponderadament cadascuna de les ofertes presentades, serà necessari que les ofertes adjuntin **l'Annex 3** correctament emplenat, amb l'objectiu que es pugui valorar que les ofertes compleixen tots i cada un dels requeriments mínims demanats.

Tanmateix, és necessari que les Memòries siguin concretes i concises amb la mínima extensió possible que permeti la clara comprensió de la proposta aportada. No s'ha d'incloure documentació o informació comercial genèrica si no aporta valor a l'oferta concreta.

7 CRITERIS D'ADJUDICACIÓ

7.1 OFERTA TÈCNICA (SOBRE B)

Es verificarà el compliment dels requeriments mínims d'acord amb l'epígraf 3 del plec i el document de l'Annex 3.

7.2 OFERTA ECONÒMICA (SOBRE C)

La valoració de les proposicions de contingut econòmic i de criteris objectius o automàtics, es durà a terme per l'aplicació dels següents criteris de valoració:

7.2.1 Preu (fins a 60 punts)

Es valorarà el preu de sortida de la següent manera:

L'oferta més econòmica, sempre i quan compleixi els requeriments tècnics mínims indicats en el plec de prescripcions tècniques, obtindrà 60 punts.

Les restants ofertes obtindran la puntuació que resulti de l'aplicació de la següent fórmula:

$P_v = \left[1 - \left(\frac{O_v - O_m}{IL}\right) \times \left(\frac{1}{M}\right)\right] \times P$	**Pv** = Puntuació de l'oferta a valorar **P** = Punts criteri econòmic = **60** **Om** = Oferta millor **Ov** = Oferta a valorar **IL** = Import de licitació **M** = Factor de modulació = 1,6

7.2.2 Altres criteris de valoració objectius (màxim 40 punts)

7.2.2.1 Experiència prèvia en integració amb el SOC de l'Agència de Ciberseguretat de Catalunya (fins a 10 punts)

Es valorarà l'experiència acreditable en projectes d'integració de l'eina de detecció i resposta amb el SIEM del SOC de l'Agència de Ciberseguretat de Catalunya.

Les referències aportades es poden acreditar mitjançant una declaració responsable, però en la fase de valoració d'aquest apartat, l'IAS podrà demanar el certificat signat pels responsables de les empreses on s'acrediti que el licitador ha executat els serveis que s'estan valorant.

L'aplicació de la puntuació es farà en base a aquesta taula:

	Número refs.	Puntuació
Referències d'integració amb el SIEM del SOC de l'ACC	cap	0
	1	3
	2	6
	3 o més	10

7.2.2.2 Referències en altres clients del sector salut de Catalunya (fins a 10 punts)

Es valorarà l'experiència demostrable d'altres instal·lacions i entrega de servei en proveïdors de salut del sistema sanitari català, en projectes de les mateixes característiques que el que es licita en el present procés de contractació.

Les referències aportades es poden acreditar mitjançant una declaració responsable, però en la fase de valoració d'aquest apartat, l'IAS podrà demanar el certificat signat pels responsables de les empreses on s'acrediti que el licitador ha executat els serveis que s'estan valorant.

	Número refs.	Puntuació
Referències en altres clients del sector salut de Catalunya	cap	0
	1	2
	2	4
	3	6
	4	8
	5 o més	10

7.2.2.3 Puntuació obtinguda en l'avaluació de MITRE (Turla 2023) (fins a 10 punts)

Es valorarà el comportament de l'eina en les avaluacions de MITRE ATT&CK (https://attackevals.mitre-engenuity.org/results/enterprise?evaluation=turla&scenario=1). Es valorarà l'eina en l'avaluació de 2023 (Turla) en els escenaris de Carbon i Snake sobre el total de 143 steps. Només es tindran en compte els resultats sense canvis de configuració ("Configuration Change" igual a NO) i sense intervenció humana ("Delayed" igual a NO), i es considerarà detectat el pas de l'atac en les categories "Technique", "Tactic" i "Telemetry".

La valoració en punts de l'avaluació obtinguda en MITRE es farà segons la següent taula:

	Número de passos	Puntuació
Del total de 143 passos de l'avaluació de l'escenari, nombre de passos detectats amb categoria "Technique", "Tactic" i "Telemetry".	>140	10
	130-139	9
	120-129	8
	100-119	7
	< 100	0

7.2.2.4 Mida de l'agent (fins a 10 punts)

Es valorarà que els paquets d'instal·lació dels agents siguin el més lleugers possible. Per aquest motiu es valorarà la mida del paquet d'instal·lació de l'agent en la seva versió per a estacions Windows d'acord amb la següent taula:

Mida en MB del paquet d'instal·lació per a Windows	Puntuació
< 20 MB	10
21 MB – 100 MB	8
101 MB – 200 MB	6
201 – 300 MB	4
301 – 400 MB	2
> 401 MB	0

8 DADES DE CONTACTE

Per a qualsevol dubte de caràcter tècnic relacionat amb aquest Plec de Prescripcions Tècniques, aclariment o visita tècnica es pot contactar amb la Direcció de sistemes d'informació al telèfon 972 18 90 25 (a l'atenció de Daniel Garcia Asquerda) o per correu electrònic: dsi.ias@gencat.cat

Per a qualsevol dubte, aclariment de caràcter jurídic o administratiu, es podrà contactar amb la responsable de Contractació Administrativa Pública de l'IAS (M.Jesús Costa Serra) per telèfon 972 18 25 09 o per correu electrònic : mariajesus.costa.ias@gencat.cat.

Salt, a 18 d'octubre de 2024

Daniel Garcia Asquerda

Director de Sistemes d'Informació de l'IAS