

Plec de prescripcions tècniques particulars que regeix la contractació basada d'un servei de Suport pel Desenvolupament d'un analista virtual

Exp. CB25AMOPL2B002

Índex

1	Introducció	4
2	Descripció dels serveis objecte de la contractació basada.	6
2.1	Context dels serveis objecte de la licitació.	6
2.2	Lot 1: serveis	6
2.2.1	Objecte i abast dels serveis.	6
2.2.2	Característiques del servei.	8
2.2.3	Volumetries	9
3	Condicions d'execució del servei	10
3.1	Horaris	10
3.2	Localització física.	10
3.3	Equip de treball	10
3.3.1	Perfils	12
3.4	Canvi de recurs	14
3.5	Control de rotació	14
3.6	Eines i equipament per a la prestació de serveis	14
3.7	Gestió del coneixement	15
3.8	Seguretat Corporativa	16
3.9	Control de Gestió	16
3.10	Documentació.	17
3.11	Formació	17
3.12	Contingència	17
3.13	Metodologia, estàndards i lliurables	18
3.14	Seguretat	18
3.11.1.	Deure de confidencialitat	18
3.11.2.	Dades de caràcter personal	18
3.11.3.	Compliment del marc legal de ciberseguretat i del marc normatiu intern	18
3.11.4.	Capacitat tècnica	19
3.11.5.	Adquisició de productes/eines i productes o serveis de seguretat	19
3.11.6.	Interconnexions	20
3.11.7.	Verificació del compliment i auditoria	20
3.11.8.	Incidents de seguretat	20
3.11.9.	Accés a la informació	20
3.12.	Assegurament i control de la qualitat i la millora contínua	21
3.13.	Seguiment del servei	21
3.14.	Integració amb altres equips	22

2	<u>Descripció dels serveis objecte de la contractació basada.</u>	6
2.1	<u>Context dels serveis objecte de la licitació.</u>	6
2.2	<u>Lot 1: serveis</u>	6
2.2.1	<u>Objecte i abast dels serveis.</u>	6
2.2.2	<u>Característiques del servei.</u>	8
2.2.3	<u>Volumetries</u>	9
3	<u>Condicions d'execució del servei</u>	10
3.1	<u>Horaris</u>	10
3.2	<u>Localització física.</u>	10
3.3	<u>Equip de treball</u>	10
3.3.1	<u>Perfils</u>	12
3.4	<u>Canvi de recurs</u>	14
3.5	<u>Control de rotació</u>	14
3.6	<u>Eines i equipament per a la prestació de serveis.</u>	14
3.7	<u>Gestió del coneixement</u>	15
3.8	<u>Seguretat Corporativa</u>	16
3.9	<u>Control de Gestió</u>	16
3.10	<u>Documentació.</u>	17
3.11	<u>Formació</u>	17
3.12	<u>Contingència</u>	17
3.13	<u>Metodologia, estàndards i lliurables</u>	18
3.14	<u>Seguretat</u>	18
3.11.1.	<u>Deure de confidencialitat</u>	18
3.11.2.	<u>Dades de caràcter personal</u>	18
3.11.3.	<u>Compliment del marc legal de ciberseguretat i del marc normatiu intern</u>	18
3.11.4.	<u>Capacitat tècnica</u>	19
3.11.5.	<u>Adquisició de productes/eines i productes o serveis de seguretat</u>	19
3.11.6.	<u>Interconnexions</u>	20
3.11.7.	<u>Verificació del compliment i auditoria</u>	20
3.11.8.	<u>Incidents de seguretat</u>	20
3.11.9.	<u>Accés a la informació</u>	20
3.12.	<u>Assegurament i control de la qualitat i la millora contínua</u>	21
3.13.	<u>Seguiment del servei</u>	21
3.14.	<u>Integració amb altres equips</u>	22
}		

1 Introducció

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència), establerta sota el marc de la Llei 15/2017, del 25 de juliol, és l'entitat que lidera i coordina els esforços de la Generalitat de Catalunya en la protecció de la informació i les infraestructures del país davant les ciberamenaces. En un món digitalitzat i interconnectat, la seguretat de la informació s'ha convertit en una prioritat estratègica, i l'Agència subratlla el compromís de Catalunya amb la promoció d'un entorn digital segur i de confiança.

Amb un enfocament clar en la prevenció i detecció de ciberamenaces, la resposta efectiva davant incidents de ciberseguretat, la promoció de la cultura de ciberseguretat, i la col·laboració i coordinació amb diferents actors a nivell local i internacional, l'Agència opera dins de l'àmbit d'actuació definit per la llei, que marca les directrius d'actuació de l'Agència, les seves funcions, estructura orgànica i el règim de governança.

L'Agència sota la direcció estratègica del Govern de la Generalitat de Catalunya, en coordinació amb les entitats del sector públic de l'Administració de la Generalitat de Catalunya, i col·laborant amb governs locals de Catalunya, sector privat i societat civil és l'encarregada d'establir i de liderar el servei públic de ciberseguretat i té com a objectiu garantir una Societat de la Informació segura i fiable per al conjunt de la ciutadania catalana i de la seva Administració Pública, amb la voluntat d'esdevenir un referent a nivell nacional i internacional en matèria de ciberseguretat.

Els avenços impulsats per l'Estratègia 2019-2022 han establert un sòlid punt de partida per a futures accions, incloent la consolidació de l'Agència de Ciberseguretat com a entitat de referència. Aquests avenços no només han millorat la capacitat de resposta davant incidents sinó que també han promogut una major consciència i formació en ciberseguretat entre la ciutadania i les organitzacions. La nova Estratègia 2023-2027, "Una Catalunya Cibersegura en una Europa Digital", s'orienta cap a reforçar la resiliència digital, protegir els serveis i infraestructures essencials, i assegurar que ciutadans i organitzacions es beneficiïn de tecnologies digitals de confiança.

En el marc de l'activitat gestionada per l'Agència de Ciberseguretat, cal destacar que *segons recull la memòria de l'Agència de Ciberseguretat de Catalunya de 2023, l'entitat ha tingut un paper rellevant en les tasques de resposta i coordinació per a la gestió d'incidents de seguretat durant el 2023, tant pel que fa a la Generalitat com en diferents entitats del territori català*. En aquest sentit, l'Agència gestiona més de 2.200 sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants. Aquest perímetre protegit provoca un alt nivell d'activitat de gestió. Més concretament, el nombre de ciberatacs rebuts durant l'any 2023 va ser de més de 5.000 milions, en contraposició als 4.400 milions d'atacs del 2022. Pel que fa als incidents de seguretat, l'Agència en va gestionar prop de 2.670 durant el 2023, en comparació amb els 2.175 de l'exercici anterior.

Les xifres fan paleses la necessitat de dotar-se de noves eines i de seguir ampliant el perímetre d'actuació. En aquest sentit, i alineat amb la nova Estratègia, l'Agència ampliarà el seu perímetre d'actuació i per tant, incrementar el nivell de protecció, resiliència i prevenció de més àmbits.

Aquest contracte està finançat per Fons Europeus. El programa RETECH constitueix un dels nous eixos transversals de l'Agenda España Digital 2026 promoguts pel Ministerio de Asuntos Económicos y Transformación Digital, i està alineat amb dues de les principals fites de l'Agenda, com són, liderar la transformació digital de manera inclusiva i sostenible i focalitzar els esforços de digitalització en sectors econòmics clau. L'objectiu del Programa RETECH és impulsar xarxes territorials

d'especialització tecnològica, articulant projectes regionals que s'orientin a la transformació i especialització digital, assegurant la coordinació, la col·laboració i la complementarietat.

Gràcies a aquest nou eix de l'Agenda España Digital 2026, es pretén liderar un canvi disruptiu, de manera inclusiva i sostenible, focalitzant els esforços de digitalització en sectors econòmics clau. En definitiva, la iniciativa RETECH permetrà impulsar els projectes tractors proposats per les Comunitats i Ciutats Autònomes, fomentant l'intercanvi de coneixement i multiplicant les oportunitats de cada regió, a través de xarxes d'impacte nacional que permetin maximitzar l'equilibri territorial i la cohesió social entre elles.

Per fer efectiva la iniciativa RETECH amb total transparència i igualtat d'oportunitats per a totes les Comunitats i Ciutats Autònomes interessades, el Ministerio de Asuntos Económicos i Transformación Digital, a través de la Secretaria d'Estado de Digitalitzación e Inteligencia Artificial, va llançar una invitació pública destinada al desenvolupament de propostes de cooperació per finançar iniciatives emblemàtiques d'especialització territorial tecnològica dins de les seves competències.

2 Descripció dels serveis objecte de la contractació basada.

2.1 Context dels serveis objecte de la licitació.

El servei objecte de licitació en aquest plec està contextualitzat en l'expedient AM.02.2024 que regeix l'Acord Marc de serveis de suport a les funcions de Ciberseguretat pròpies del Centre d'Operacions de Seguretat de l'Agència de Ciberseguretat de Catalunya.

Concretament s'emmarca en el:

Lot 2: Enginyeria de seguretat

Dins d'aquest lot s'inclouen, tal i com indica el Plec de Clàusules Tècniques de l'Acord Marc de referència, el suport en les tasques d'administració i manteniment de les solucions tecnològiques de seguretat emprades per l'Agència de Ciberseguretat en els diferents àmbits per poder donar una resposta adequada a les funcions que han de desenvolupar els diferents serveis i necessitats de l'Agència, tant en la correcta posada a punt com a les necessitats funcionals.

Actualment, la Generalitat de Catalunya rep més de 7.000.000.000 atacs contra la seva infraestructura i sistemes d'informació, els quals en la majoria dels casos té com a objectiu posar en risc la disponibilitat, integritat i/o confidencialitat dels serveis públics de Catalunya.

Amb aquest context, és fonamental garantir les capacitats necessàries per poder realitzar una gestió eficient i eficaç davant aquesta activitat, identificant el més ràpid possible quina d'aquesta activitat és un incident potencial i requereix executar tasques de protecció o resposta per evitar l'afectació en processos crítics a la ciutadania. Per aquest fet, i amb l'objectiu de reduir els temps de detecció i resposta davant atacs i incidents de seguretat, aquest projecte persegueix desenvolupar automatitzacions de nivell 1 les quals, mitjançant els principals playbooks de gestió d'atacs i incidents de ciberseguretat, redueixin els temps de detecció, anàlisi i protecció de potencials ciberincidents, i incrementar de forma rellevant el grau de seguretat dels serveis públics de la Generalitat de Catalunya.

2.2 Lot 1: serveis

2.2.1 Objecte i abast dels serveis.

L'objecte de la present licitació és la contractació d'un servei de suport pel desenvolupament d'automatitzacions de processos que permetin millorar l'eficiència operativa de l'Àrea d'operació de la seguretat (en endavant, AOS) garantint un impacte positiu en la ciutadania al millorar el temps de detecció i resposta en els ciberatacs i per tant reduint la finestra d'exposició.

Les automatitzacions desenvolupades hauran de permetre:

- Enriquiment de les alertes de seguretat.
- Automatització de la classificació, primera contenció i remediació parcial d'incidents de ciberseguretat.
- Integració amb les eines de detecció i resposta del SOC. (SIEM, SOAR, EDRs, NGFW, etc)
- Reducció del temps de resposta davant ciberatacs i optimització dels recursos del SOC.
- Correlació d'alertes per identificar amenaces complexes i persistents.

- Generació d'informes automatitzats amb l'estat dels incidents i les accions realitzades.
- Escalat automàtic d'incidentes crítics als analistes de nivell 2/3.

Tot seguit es descriuen les principals activitats i funcionalitats que s'esperen:

Enriquiment de les alertes de seguretat.

Millora en el context de les alertes mitjançant la incorporació automàtica d'informació, com ara dades d'intel·ligència d'amenaces, geolocalització, reputació d'IPs i històric d'incidentes, etc.

Les automatitzacions han de correlacionar dades internes i externes per facilitar una avaluació més precisa i prioritzar les amenaces més crítiques.

Automatització de la classificació, primera contenció i remediació parcial d'incidentes de ciberseguretat.

Implementació de playbooks automatitzats per categoritzar alertes segons la gravetat, tipologia i origen, accelerant així l'anàlisi inicial i primera resposta.

Ha de poder executar accions de contenció, com l'aïllament d'equips compromesos o el bloqueig d'IPs sospitoses, i aplicar mesures de remediació bàsiques.

Integració amb les eines de detecció i resposta del SOC

Connexió amb les principals plataformes de detecció i resposta per garantir la recepció d'alertes en temps real i l'execució d'accions automatitzades.

Reducció del temps de resposta davant ciberatacs i optimització dels recursos del SOC.

Automatització de tasques repetitives per minimitzar el temps dedicat a l'anàlisi manual i accelerar la resposta davant incidents crítics.

Ha de millorar l'eficiència operativa permetent que els analistes se centrin en investigacions avançades i la resolució d'amenaces complexes.

Correlació d'alertes per identificar amenaces complexes i persistents.

Capacitat per correlacionar múltiples alertes d'origens diferents per detectar patrons d'atac sofisticats que podrien passar desapercebuts individualment.

Ha d'utilitzar tècniques d'anàlisi avançat per identificar activitats sospitoses persistents i alertar en cas d'indicadors de compromís (IoCs).

Generació d'informes automatitzats amb l'estat dels incidents i les accions realitzades.

Creació automàtica d'informes detallats que resumeixin la naturalesa de l'incident, les accions dutes a terme i l'estat actual de la remediació.

Ha de permetre la personalització dels informes segons el públic destinatari (analistes, responsables de seguretat o direcció).

Escalat automàtic d'incidentes crítics als analistes de nivell superior.

Identificació d'incidents d'alta gravetat o complexitat i derivació automàtica a l'equip de nivell 2 o 3 per a una revisió més exhaustiva.

Les automatitzacions desenvolupades han de garantir que els incidents crítics no es quedin sense atenció, aplicant criteris definits per a l'escalat automàtic.

2.2.2 Característiques del servei.

De tot el que s'ha exposat prèviament es pot observar com, a l'hora de presentar les seves ofertes, els licitadors han de tenir en compte els següents elements essencials:

Gestió integral del projecte i coordinació amb stakeholders

El servei ha d'incloure la gestió completa del projecte, garantint una coordinació eficient amb tots els stakeholders implicats. Això inclou:

- **Gestió i coordinació de les integracions** amb les eines de seguretat existents (SIEM, SOAR, EDR, NGFW, etc.), assegurant-ne la compatibilitat i correcte funcionament.
- **Comunicació constant amb els equips operatius** per entendre els requisits, validar funcionalitats i garantir un alineament continu amb les necessitats del SOC.
- **Priorització de tasques i planificació** del desplegament de funcionalitats, assegurant que les fases del projecte es desenvolupin de manera estructurada i eficient.

Desenvolupament i validació de les automatitzacions

El servei ha d'incloure el desenvolupament i implementació de les automatitzacions necessàries per a la detecció, resposta i gestió d'incidents. Això implica:

- **Creació de playbooks automatitzats** per a la classificació, contenció i remediació d'incidents, basant-se en les millors pràctiques del sector.
- **Execució de proves i validació** de les automatitzacions per garantir que les accions realitzades compleixen els requeriments i necessitats operatives del SOC.
- **Monitorització i ajust continu** de les automatitzacions per assegurar una resposta efectiva davant de noves amenaces o canvis en l'entorn del SOC.

El servei no només inclou l'automatització tècnica, sinó també tota la gestió i alineament amb els equips operatius per garantir-ne l'èxit.

Arquitectura de la solució

Cal tenir present que la solució d'automatització, orquestració i resposta de seguretat desplegada a l'Àrea d'operacions de l'Agència de Ciberseguretat de Catalunya és Cortex XSOAR de l'empresa Palo Alto Networks. En conseqüència, el desplegament del servei objecte d'aquest basat, haurà de ser sobre aquesta solució tecnològica.

Suport tècnic fabricant

Amb l'objectiu de garantir l'èxit del projecte, així com assegurar la correcta implantació de les automatitzacions segons les millors pràctiques del fabricant, l'adjudicatari haurà d'aportar un mínim de 200 hores de suport tècnic especialitzat proporcionat directament per Palo Alto Networks. Aquestes hores hauran de destinar-se a tasques com la revisió d'arquitectura, l'assessorament en el

disseny i desplegament de playbooks, la validació funcional de les automatitzacions i el suport avançat durant les fases crítiques del projecte. Aquesta col·laboració directa garantirà un desplegament més fluid, eficient, segur i optimitzat per a les necessitats específiques de l'àrea d'operacions, aprofitant al màxim les capacitats de la plataforma i assegurant un suport expert en cas de necessitat.

2.2.3 Volumetries

El nombre total de processos a automatitzar (playbooks) és de 50. S'ha dimensionat una mitja de 120h per cadascun d'aquest playbooks, resultant un total de 6.000 hores de desenvolupament necessari.

3 Condicions d'execució del servei

3.1 Horaris

El servei s'haurà de prestar d'acord amb els horaris de prestació dels serveis de l'Agència, 8x5 en horari de dies laborables. Es considera horari de dies laborables els dies que siguin laborables al centre de treball de l'Hospitalet de Llobregat amb prestació de 9:00h a 18:00h.

A petició expressa de l'Agència, es podrà requerir la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei. Aquestes tasques poden incloure activitats crítiques descrites a l'objecte del contracte. Sovint, aquestes accions s'han de dur a terme fora de l'horari habitual per evitar interferències amb l'operativa ordinària de l'Agència, minimitzar riscos en serveis productius i garantir la disponibilitat continuada dels sistemes. Així mateix, l'assistència a comitès de crisi també poden requerir intervencions en moments no laborables, especialment en entorns amb alts requeriments de seguretat i continuïtat operativa.

Si durant l'execució del contracte l'Agència o l'adjudicatari detecten la necessitat de modificar l'horari del servei o equip descrit en aquest plec, l'Agència i l'adjudicatari consensuaran de forma conjunta la modificació, essent l'Agència qui finalment designi l'horari de prestació que s'adeqüi a les necessitats pròpies i que no perjudiqui de forma excessiva a l'adjudicatari.

3.2 Localització física.

Inicialment, els equips prestataris dels serveis estaran ubicats físicament a les oficines de l'adjudicatari o en alguna altra que ambdues parts acordin, atenent sempre a la seguretat de la informació gestionada pel servei. Tot i això, l'Agència considera que l'adjudicatari, en coordinació amb la Direcció de l'àrea de l'Agència, podria arribar a prestar/executar fins al 50% de les tasques/projectes/serveis amb recursos ubicats a les instal·lacions de l'Agència de Ciberseguretat a l'Hospitalet de Llobregat.

Addicionalment, s'ha de contemplar la possibilitat que part d'aquests serveis requereixin del desplaçament dels professionals a les instal·lacions dels clients de l'Agència que poden estar ubicades a qualsevol part del territori de Catalunya.

Al llarg del contracte es podria requerir un canvi tant en la ubicació dels professionals, com la presència de l'equip a les instal·lacions de l'Agència, d'acord amb les necessitats dels serveis i l'organització d'equips de treball. En cap cas la ubicació dels professionals suposarà un increment dels costos vinculats a la prestació dels serveis.

3.3 Equip de treball

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos de l'adjudicatari del contracte basat amb la qualificació necessària i adequada per a la prestació del servei.

Els mitjans personals necessaris per a la prestació dels serveis han de ser els adequats per realitzar amb garantia les tasques definides i han de mostrar les habilitats necessàries per tal d'integrar-se en un equip d'alt rendiment, entre les quals es podrien determinar a efectes enunciatius les següents:

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.

- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.
- Habilitat per identificar, analitzar i resoldre problemes.
- Capacitat de treball sota pressió.
- Coneixement de català, castellà i d'anglès, parlat i escrit.
- Ampli coneixement legal, tecnològic i de negoci de seguretat informàtica i de l'entorn de l'administració pública.
- Altres necessaris per al bon desenvolupament dels serveis.

El licitador proposarà un equip de treball (descrivint-ne els perfils, dedicació, pla de treball, etc.) per a l'execució dels serveis sol·licitats en el present plec, d'acord amb les condicions i paràmetres esmentats en els apartats d'aquest plec.

No es preveu la possibilitat de transferència del personal intern de l'Agència o dels seus clients.

L'adjudicatari disposarà d'una figura que assumirà les tasques de cap de servei. A aquest efecte, ha d'assumir les següents responsabilitats addicionals a les descrites a l'acord marc on s'emmarca el present basat:

- Actuar com a interlocutor de l'empresa adjudicatària, canalitzant la comunicació entre l'empresa adjudicatària i el personal integrant de l'equip de treball adscrit al contracte d'una banda, i de l'altra, en totes aquelles qüestions derivades de l'execució del contracte.
- Distribuir el treball entre el personal encarregat de l'execució del contracte, e impartir als esmentats treballadors les ordres o instruccions de treball que resultin necessaris en relació a la prestació del servei contractat.
- Supervisar el correcte desempeñament per part del personal integrant de l'equip de treball de les funcions que tenen encomanades, així com controlar l'assistència d'aquest personal al lloc de treball.
- Organitzar el règim de vacances del personal adscrit a l'execució del contracte, havent-se de coordinar amb el responsable del contracte a tal efecte de forma adequada per tal de no alterar el funcionament del servei.
- Informar al responsable del contracte sobre les vacances, ocasionals o permanents, en la composició de l'equip de treball adscrit a l'execució del contracte.

Per dur a terme aquestes tasques, aquest perfil hauria de posseir coneixements i experiència en:

- Definició i millora de processos.
- Eines de reporting i quadres de comandament.
- Tecnologies aplicades a centres d'operació de la seguretat
- Marcs normatius i metodològics més comuns de gestió (ITIL, ISO 20000, Prince2, COBIT, PMP o similar) i de seguretat (ISO27000, NIST o similar)
- Experiència contrastada en gestió de projectes i serveis de seguretat de la informació, incloent Ciberseguretat.
- Experiència demostrable en desplegament, gestió i direcció de serveis de Ciberseguretat.

Aquesta figura haurà de ser assumida pel membre que compleix amb el Perfil coordinador de l'automatització que es descriu més endavant. És a dir, no s'ha d'ofertar un perfil propi de cap de servei, sinó que aquestes funcions s'assignaran a un dels membres mínims requerits.

Els licitadors hauran d'incloure en la seva proposta l'organigrama i esquemes d'equips per tal de donar resposta a les necessitats expressades en aquest plec.

Per raons d'operativitat, de coneixement de les tasques a realitzar i de sensibilitat de la informació amb la que es treballa, cal garantir al màxim la continuïtat de l'equip que donen servei a l'Agència.

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **12.336 hores amb un període d'execució de 9 mesos**, essent com a màxim fins el 30 de juny de 2026. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	Hores anuals mínimes estimades
Perfil coordinador de l'automatització	3.168 hores
Perfil enginyer d'automatització	6.000 hores
Perfil validador de seguretat	3.168 hores

Els requisits anteriors s'han d'entendre com a mínims aproximats, podent els licitadors ampliar-los i millorar-los a les seves ofertes.

3.3.1 Perfils

Els requeriments mínims dels perfils professionals que poden composar l'equip són els següents:

PERFIL	REQUISITS
Perfil coordinador de l'automatització	- Experiència professional mínima de 5 anys en gestió de projectes. - Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. - Certificat en: Project Management Professional (PMP), Certified Associate in Project Management (CAPM), PRINCE2 (Projects IN Controlled Environments), AgilePM, per part d'un integrant de l'equip. - Haver participat i poder demostrar la seva involucració en mínim un projecte en els que hagi desenvolupat les següents funcions: - Lideratge de projectes i equips de treball multidisciplinars. - Gestió i seguiment de projectes (incloent la identificació i validació de requeriments, gestió de riscos, identificació i control de desviaments de terminis, etc.) - Coneixements en: - Definició i millora de processos. - Gestió de projectes (metodologies, processos, eines, lliurables, etc.). - Eines de reporting i quadres de comandament.

	•Tecnologies aplicades a centres d'operació de la seguretat (SOCs). ▪ Marcs metodològics més comuns de gestió (ITIL, ISO 20000, Prince2, COBIT, PMP o similar) i de seguretat (ISO27000, NIST o similar).
Perfil enginyer d'automatització	• Experiència professional mínima de 5 anys en projectes de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Especialista en Implementació i administració automatitzacions en eines SIEM/SOAR. • Certificat en: Palo Alto Network Security Automation Engineer (PCSAE), Palo Alto Networks Micro-Credential for Cortex XSOAR Consultant (PMXrC), per part d'un integrant de l'equip. • Haver participat i poder demostrar la seva involucració en mínim un projecte en els que hagi desenvolupat les següents funcions: ▪ Lideratge i gestió de projectes i equips de treball multidisciplinars. ▪ Gestió i operació de serveis de SOC. ▪ Projectes d'automatització i industrialització. ▪ Automatització de tasques operatives recurrents. ▪ Desenvolupament i consum d'APIs. ▪ Desenvolupament full stack multi plataforma. ▪ Desenvolupament de Backend WEB y API REST. • Coneixements en: ▪ Llenguatges de programació, especialment Python, Ruby, Javascript i Perl. ▪ Principals amenaces i vectors d'atac que afecten a les organitzacions (per exemple, el catàleg d'amenaces que proposa l'organització NIST). Habilitats comunicatives avançades i capacitat de coordinació i interlocució amb altres equips.
Perfil validador de seguretat	• Experiència professional mínima de 5 anys en projectes de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Coneixements tècnics en elements de seguretat, sistemes operatius, xarxes, protocols i programari. • Coneixements a nivell analític per abastar tot l'escenari d'un incident • Coneixements tècnics en investigació i anàlisi d'amenaces i atacs. • Coneixements tècnics dels elements de seguretat. • Coneixements relacionats amb l'aplicació de metodologies i operació d'eines de monitorització i protecció perimetral. • Coneixements per al tractament i resposta davant d'esdeveniments i incidents de seguretat.

S'entén que aquests perfils es corresponen amb els rols que, des de l'Agència, s'identifiquen per la prestació d'aquest servei, deixant a la banda dels licitadors la proposta de desplegament, composició de l'equip, adequació de perfils i dedicació global dels mateixos.

3.4 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte basat el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies laborables a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència a l'empresa adjudicatària del contracte basat. L'adjudicatari haurà de presentar en un termini màxim de 10 dies laborables a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució. Si l'objecte del contracte basat ho requereix, aquest aspecte es podrà concretar en aquest.

3.5 Control de rotació

L'estabilitat dels recursos del servei amb coneixement i compromís és molt important per a la correcta prestació del servei.

L'empresa adjudicatària del contracte basat podrà fer canvis en l'equip de treball durant l'execució del contracte, però ho haurà de notificar per escrit a l'Agència amb una antelació mínima de 14 dies naturals, justificant el canvi i informant del perfil i característiques de la persona que s'incorpora. L'Agència comprovarà que la persona a incorporar compleix amb les condicions curriculars del component de l'equip que substitueixi.

L'empresa assumirà la selecció de les persones de nova incorporació, la coexistència en el servei del personal sortint i l'entrant sense cost per l'Agència, assegurant el correcte traspàs de coneixement en els següents 15 dies i duent a terme els controls necessaris per garantir-lo entenent, per tant, la no facturació d'aquests dies d'adaptació i traspàs. Sens perjudici que si s'escau es puguin aplicar els ANS corresponents per rotació excessiva.

En cap cas la substitució de personal suposarà un cost addicional, havent-se de garantir que el servei no es vegi afectat per aquest canvi. Si l'objecte del contracte basat ho requereix, aquest aspecte es podrà concretar en el contracte basat.

3.6 Eines i equipament per a la prestació de serveis.

Les principals eines requerides (gestió d'esdeveniments, alertes, sistema de registre, anàlisi de codi, web i infraestructura...) per la prestació del servei seran proporcionades per l'Agència. El licitador haurà de fer servir aquestes eines, no podent extreure informació fora de l'àmbit d'actuació per la seva manipulació o explotació sense autorització prèvia de l'Agència.

Quan l'adjudicatari es trobi en les instal·lacions de l'Agència, proveirà a les persones que prestin els serveis:

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l'Agència.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides l'Agència.
- Telefonia fixa a les instal·lacions del servei.

- Telefonia mòbil per donar cobertura als serveis de guàrdia.
- Accés a Internet a través de la xarxa d'àrea local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.

L'Agència no proveirà:

- Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina ni tampoc ordinadors portàtils amb el programari habitual de l'Agència.
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.
- Accés a Internet via GPRS, UMTS.
- Cap altre recurs no especificat explícitament.

En conseqüència, els adjudicataris hauran de:

- Subministrar tots elements de maquinari, programari i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments de l'objecte del contracte. Aquests elements seran d'ús exclusiu pels serveis prestats a l'Agència i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.
- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.
- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip de Mitjans Tècnics de l'Agència.

L'Agència es troba en un procés de revisió i millora contínua que pot implicar la realització de canvis importants en el referent a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei.

Per aquest motiu és imprescindible que l'adjudicatari tingui presents les següents consideracions en el referent a les eines de gestió durant l'execució del contracte.

- L'Agència decidirà la utilització de qualsevol tecnologia nova o evolució de les existents, relacionades amb la prestació del servei.
- L'Agència decidirà la forma d'implantar qualsevol d'aquests nous sistemes, planificar els projectes corresponents i el seu calendari, així com la transició des dels sistemes existents cap als nous.
- Els adjudicataris es comprometen a assumir i adaptar-se a aquestes noves tecnologies i sistemes per donar el servei de suport, així com participar activament en el procés de transició, formant i preparant el seu personal en aquestes noves tecnologies i sistemes implantats sense cost addicional per l'Agència.

3.7 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions com a Centre d'Innovació i Competència en Ciberseguretat (CIC4Cyber) i, especialment, l'impuls de la transformació fonamentada en el coneixement col·laboratiu, la coordinació de l'ecosistema de ciberseguretat i la voluntat per la innovació contínua, es requereix que l'empresa adjudicatària registri tot el coneixement que disposi i es generi en la contractació basada que derivi del present Acord Marc d'acord amb les directrius del CIC4Cyber.

A tal efecte, l'adjudicatària haurà de mantenir aquest coneixement actualitzat i accessible per a l'organització, havent de proporcionar una descripció detallada del coneixement que es disposi i es generi al servei ofert, i tenint, per part de l'organització, accés a aquest coneixement en qualsevol moment.

3.8 Seguretat Corporativa

Un cop adjudicat el contracte basat, tant l'empresa adjudicatària s'haurà de sotmetre a les polítiques i regulacions internes que estableix l'àrea de Seguretat Corporativa en matèria de seguretat de la informació, com a mínim i no limitant-se a:

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- Facilitar l'accés en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de l'Agència (sigui o no per l'exercici de la seva funció).
- Acceptar les normes i polítiques que estableix l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.
- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'àrea de Mitjans Tècnics per fer el desplegament de polítiques i controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.
- Els equips, així com la informació resident dels mateixos serà sempre custodiada per l'Agència.
- Garantir l'estabilitat dels equips (reduint al mínim la rotació de personal).
- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (ENS, LOPDGDD, GDPR, LSSI, etc.).

A la finalització del contracte, l'adjudicatari del contracte basat quedarà obligat al lliurament o destrucció en cas de ser sol·licitada, de qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

3.9 Control de Gestió

L'empresa adjudicatària del contracte basat, i en especial el cap de servei, haurà de col·laborar amb el responsable de la planificació pressupostària i el control de gestió de l'Agència per tal:

- De complir amb el model de seguiment econòmic i planificació en termes de capacitat i execució de tasques.
- D'ajustar-se als procediments de facturació que determini l'Agència.
- De conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència, d'acord amb els procediments establerts.
- D'exercir la gestió del contracte amb capacitats de *forecast*.

- Realitzar el *reporting* en les eines proporcionades per l'Agència amb els següents conceptes.
- Fitxer mestre de persones.
- Fitxer mestre de projectes i activitats.
- Estimació de recursos per projecte.
- Seguiment dels riscos.
- Seguiment del consum de recursos.
- Imputació de temps i activitats.
- Assignació de tasques a persones.
- Memòria d'activitat del contracte.
- Facturació i Conformació de factures.

L'adjudicatari proporcionarà la seva total col·laboració per a la realització d'auditories i la verificació del compliment dels compromisos. Aquestes auditories, realitzades en qualsevol de les instal·lacions involucrades en la prestació del servei, podran ser portades a terme per personal de l'Agència o sol·licitades a tercers. No serà necessari fer una notificació prèvia per a la realització de tasques d'auditoria que no requereixin la col·laboració activa per part del personal de l'adjudicatari. En el cas en què sigui necessària aquesta col·laboració, l'Agència farà una notificació amb dues setmanes d'antelació.

3.10 Documentació.

L'Agència és el propietari de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris i el seu personal i subcontractats que destini a l'execució dels serveis. L'adjudicatari s'encarregarà de disposar de totes les autoritzacions i permisos necessaris per tal de poder donar compliment a aquesta previsió, essent responsabilitat de l'adjudicatari qualsevol pagament o reclamació relativa a aquesta manca d'autoritzacions.

Els responsable de servei de l'Agència serà els responsable de la validació i aprovació dels documents elaborats pel personal de l'adjudicatari. En cas que la qualitat dels documents sigui molt baixa o de manera recurrent i/o perllongada en el temps de prestació dels serveis no assoleixi els nivells requerits s'aplicaran les penalitzacions establertes en la present licitació.

L'adjudicatari haurà de mantenir la documentació actualitzada en el sistema de gestió documental que l'Agència proporioni per tal efecte

3.11 Formació

El personal de l'empresa adjudicatària del contracte basat realitzarà, formació continuada per tal de garantir l'actualització dels seus coneixements així com l'adquisició de nou coneixement que pugui ser de valor pels serveis de l'Agència.

3.12 Contingència

Hauran de proveir un pla de contingència, en cas de desastre de les instal·lacions principals, en unes instal·lacions alternatives (centre de gestió secundari) propietat del licitador, que inclouran:

- Estacions de treball amb el programari adequat per realitzar les tasques descrites.

- Comunicacions d'accés a les aplicacions informàtiques.
- Telefonia fixa a les instal·lacions del servei.
- Accés a Internet a través de la xarxa d'àrea local.
- Espai suficient per allotjar en condicions de treball òptimes:
 - El personal necessari de l'adjudicatari per realitzar el servei i
 - Personal de l'Agència, o de terceres parts determinades per aquest, per a la correcta gestió del servei.
- Pla i execució de proves per validar la solució de contingència implementada, amb la periodicitat que l'Agència determini.

Les instal·lacions i equipament haurà de ser suficient per garantir la continuïtat dels serveis de l'Agència durant l'existència de la causa que doni lloc a la contingència.

3.13 Metodologia, estàndards i lliurables

L'organització del treball i execució del servei s'haurà d'adequar a les metodologies, estàndards i lliurables establerts per l'Agència vigents en el moment de l'execució del servei objecte del contracte basat.

3.14 Seguretat

En matèria de seguretat de la informació, l'empresa adjudicatària té les següents obligacions:

3.11.1. Deure de confidencialitat

Tot el personal de l'empresa adjudicatària així com els possibles subcontractistes han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat s'haurà de mantenir durant 10 anys, o el que s'especifiqui en el contracte basat, des de que es va tenir coneixement de la informació, excepte en relació a les dades personals a les que accedeixin respecte a les que caldrà mantenir el deure de confidencialitat de manera indefinida, subsistint inclús quan es finalitzi la relació contractual, segons estableix la Llei Orgànica 3/2018.

L'empresa ha de comunicar aquesta obligació de confidencialitat al seu personal ja sigui intern com extern, que estigui involucrat en l'execució del contracte i possibles subcontractistes i ha de controlar el seu compliment.

L'empresa adjudicatària ha de posar en coneixement de l'Agència, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de la informació.

3.11.2. Dades de caràcter personal

En relació amb el tractament de dades de caràcter personal, l'empresa adjudicatària del contracte basat donarà compliment com a encarregat de tractament del que estableix el Reglament General de Protecció de Dades.

3.11.3. Compliment del marc legal de ciberseguretat i del marc normatiu intern

L'empresa adjudicatària del contracte basat haurà de complir amb tots els requeriments que siguin d'aplicació d'acord amb el marc legal en matèria de ciberseguretat i amb el marc normatiu intern que siguin aplicables.

En relació al marc legal en matèria de ciberseguretat, i, en concret, al compliment de l'Esquema Nacional de Seguretat (ENS), l'empresa adjudicatària del contracte basat haurà d'assegurar la conformitat dels sistemes d'informació que sustentin la prestació de serveis o de les solucions que pugui proveir amb l'ENS durant tot el termini d'execució del contracte i, si escau, haurà d'estendre aquesta exigència a la cadena de subministrament. L'Agència de Ciberseguretat podrà requerir a l'empresa adjudicatària del contracte basat el lliurament de la documentació acreditativa de la conformitat amb l'ENS. L'empresa adjudicatària del contracte basat haurà de designar, segons estableix l'ENS, un punt de contacte per a la seguretat (POC) que canalitzarà i supervisarà el compliment dels requisits de seguretat de la informació i la gestió dels incidents que es puguin produir durant l'execució del contracte.

A més de l'ENS i la normativa i guies tècniques que el desenvolupen, l'empresa adjudicatària del contracte basat haurà de conèixer i aplicar el marc normatiu intern, que inclourà el Marc Normatiu de Seguretat la Informació de la Generalitat de Catalunya i la normativa pròpia, les directrius o instruccions de l'Agència de Ciberseguretat. Especialment haurà de complir amb la Política de seguretat aplicable i la normativa relativa a l'ús de les tecnologies de la informació i la comunicació, aprovada per Instrucció de la Secretaria d'Administració i Funció Pública i que es pot consultar al lloc web d'aquesta Secretaria. Si escau, l'empresa adjudicatària del contracte basat haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

3.11.4. Capacitat tècnica

Per a poder executar el contracte i oferir garanties de la seva capacitat tècnica, l'empresa adjudicatària del contracte basat haurà de presentar compromís exprés d'adscripció al contracte dels mitjans personals que s'especifiquin als plecs, complint amb els requeriments definits de formació, i acreditar la disposició efectiva dels mateixos.

L'empresa adjudicatària del contracte basat ha de garantir que tot el personal sigui conscienciat, rebi formació i informació sobre els seus deures, obligacions i responsabilitats en matèria de seguretat derivats de la legislació, del marc normatiu intern i dels procediments i directrius aplicables, recordant les possibles mesures disciplinàries aplicables i el seu deure de confidencialitat respecte a la informació a la que tingui accés.

3.11.5. Adquisició de productes/eines i productes o serveis de seguretat

Tant en el cas que es desenvolupin productes/eines, es facin integracions amb altres eines o s'adquireixin eines de mercat o qualsevol component de sistemes d'informació (hardware, software, etc.), aquests hauran de ser compatibles amb l'arquitectura de seguretat de l'Agència i complir amb els requeriments de seguretat que estableixi el marc legal i el marc normatiu intern, sotmetre's a proves tècniques de seguretat i aplicar les correccions necessàries prèviament a la posada en producció del producte/solució/eina. Caldrà incorporar el producte/eina dins el procés de desenvolupament segur de l'Agència de Ciberseguretat des de la fase de disseny fins a la posada en producció.

L'empresa adjudicatària del contracte basat haurà de garantir que disposa dels perfils amb la capacitat i la formació necessària per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició. A més, haurà de proporcionar formació i capacitat per al personal que designi l'Agència per tal que aquest personal adquireixi els coneixements necessaris per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició.

En cas que es contractin productes de seguretat o serveis de seguretat de les tecnologies de la informació i la comunicació que vagin a ser emprats en els sistemes d'informació de l'Agència, segons estableix l'ENS, hauran de tenir certificada la funcionalitat de seguretat relacionada amb el seu objecte d'adquisició. Els productes o serveis de seguretat hauran de constar al Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del Centre Criptològic Nacional o bé complir amb els criteris que estableixi l'Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centre Criptològic Nacional o, en el seu defecte, acreditar que el producte o servei disposa de requeriments equivalents.

3.11.6. Interconnexions

Segons preveu l'ENS, en el cas que sigui necessari realitzar interconnexions entre sistemes de l'empresa adjudicatària del contracte basat i l'Agència o amb d'altres entitats:

- No es podran dur a terme, tret que prèviament hagin estat autoritzades expressament per l'Agència.
- En cas que s'autoritzi una interconnexió, l'empresa adjudicatària del contracte basat haurà de garantir que es documentin com a mínim les característiques de la interfície, els requisits de seguretat i protecció de dades i la naturalesa de la informació intercanviada. Aquesta documentació l'haurà de facilitar a l'Agència.
- L'empresa adjudicatària del contracte basat haurà de participar en els mecanismes de coordinació que estableixi l'Agència i seguir els procediments establerts per aquest fi, per a poder atribuir i exercir de manera efectiva, les responsabilitats en relació a cada sistema interconnectat.

3.11.7. Verificació del compliment i auditoria

L'Agència es reserva el dret a verificar i auditar, amb mitjans propis o de tercers, el compliment de les mesures de seguretat requerides en base al marc legal de ciberseguretat i al marc intern per als sistemes d'informació emprats per a l'execució del contracte, en el moment i amb la periodicitat que s'estimi convenient. L'Agència podrà requerir el seguiment dels plans d'acció derivats d'aquestes verificacions i auditories. L'empresa adjudicatària del contracte basat haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en relació a aquest model de compliment, donant resposta en els terminis marcats per l'Agència de Ciberseguretat. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència de Ciberseguretat.

3.11.8. Incidents de seguretat

El POC haurà de notificar a l'Agència de Ciberseguretat qualsevol incident de seguretat que pugui redundar, directament o indirectament, en la seguretat dels sistemes d'informació, en els terminis i per les vies que determini o els procediments establerts. L'empresa adjudicatària del contracte basat haurà d'aportar tota la informació necessària per a la seva gestió i notificació als organismes competents per part de l'Agència de Ciberseguretat.

En cas que sigui necessari, l'empresa adjudicatària del contracte basat haurà de col·laborar amb qualsevol de les tasques que siguin requerides per part de l'Agència de Ciberseguretat per a la identificació, contenció, erradicació, recuperació i recopilació de les evidències dels incidents de seguretat.

3.11.9. Accés a la informació

L'empresa adjudicatària del contracte basat haurà de garantir l'accés del personal autoritzat de l'Agència de Ciberseguretat a la informació de seguretat (procediments, registre d'incidents, traces, etc.) per a poder desenvolupar l'objecte del contracte.

Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. L'Agència de Ciberseguretat i l'empresa establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.

3.12. Assegurament i control de la qualitat i la millora contínua

L'empresa ha de vetllar per l'excel·lència i millora contínua dels processos, components tècnics i serveis sota el seu abast.

Per tal de garantir que s'aborda la qualitat i la millora, l'adjudicatari haurà d'elaborar, mantenir i executar un "Pla de Qualitat i Millora Contínua" que inclogui, entre d'altres:

- Anàlisi i avaluació de les dades obtingudes de la mesura del servei, tant de producció i activitat com de gestió de l'incidental i operació.
- Plans de millora del servei orientats a millorar el compliment dels objectius del servei i del negoci.
- Accions per l'assegurament i control de la qualitat (revisions, proves, etc.), amb major rigor, intensitat i profunditat segons la criticitat del projecte/servei/component.
- Accions per reduir el nombre d'incidències, problemes freqüents i el suport.
- Accions per millorar la qualitat percebuda i la satisfacció dels usuaris.
- Accions preventives per la mitigació de riscos, tenint en compte la seva probabilitat i el seu impacte.
- Accions dirigides a millorar la gestió del coneixement i incrementar la usabilitat dels serveis.
- Accions per maximitzar l'eficiència i la sostenibilitat del servei.

3.13. Seguiment del servei

Les empreses adjudicatària haurà de presentar un informe de seguiment de cada contracte basat d'acord amb els indicadors de compliment i altra informació rellevant pel seguiment del servei. Aquests informes s'avaluaran als comitès operatius i es formalitzaran i s'elevaran els seus resultats a la resta de comitès.

L'informe de seguiment haurà de tenir, com a mínim:

- Un informe de gestió dels serveis desenvolupats per a cada basat, amb indicació de les activitats realitzades i les previstes realitzar, les volumetries globals d'activitat i els indicadors de compliment especificats als Acords de Nivell de Servei (ANS) de cada basat.
- Un informe de dedicació del basat a les diferents funcions requerides, per tal de poder avaluar la distribució dels esforços.
- Un informe d'accions de millora de l'activitat del propi basat, on es detallaran les accions de millora proposades amb informació rellevant per a la seva gestió (per exemple, el benefici previst obtenir, el termini d'implantació, etc.). Per cada millora implantada s'establirà, sempre que sigui possible, un indicador que s'afegirà a l'informe de gestió dels serveis. La periodicitat

de l'informe de seguiment serà mensual, quant al seguiment de les activitats i la implantació de les millores. La presentació de les propostes de millora es farà amb la periodicitat indicada en cada contracte basat o el que es determini per part del responsable del contracte de l'Agència de Ciberseguretat.

Si existeix cap especificitat en aquest sentit, es recollirà al basat corresponent.

Pel control i seguiment del servei s'utilitzaran dades, mètriques i informes (en endavant informació) que serviran de suport als òrgans de gestió establerts i que són, en el seu conjunt, el mecanisme de seguiment i avaluació del servei. Aquesta informació es pot fer extensible a altres Unitats, Àrees, Direccions de l'Agència o tractar-se d'anàlisi puntual.

L'empresa adjudicatària del contracte basat és la responsable de generar i lliurar la informació que es determini en els diferents àmbits del servei, la qual ha de permetre a l'Agència governar, controlar i gestionar els serveis prestats objecte del contracte, tant des d'una òptica individual, com transversal i global.

La periodicitat, dates límit de lliurament, canals de transmissió, format exacte i contingut detallat de la informació a elaborar en tots els àmbits del servei, seran definits per l'Agència. L'Agència podrà sol·licitar, durant la vigència del contracte, ampliacions i canvis en el contingut, periodicitat, canals i format de la informació per ajustar-se a les necessitats de seguiment dels serveis.

L'empresa es compromet a automatitzar tot el possible els processos de generació i transmissió de la informació, arribant a la màxima integració possible.

L'empresa es compromet a proporcionar informació veraç i contrastada, i haurà de disposar dels mecanismes necessaris per garantir-ho. L'Agència podrà dur a terme les auditories que consideri necessàries per a la seva verificació, obligant-se l'empresa a participar-hi de manera activa i diligent sense cap cost afegit per a l'Agència.

L'Agència podrà sol·licitar informació de forma immediata i l'empresa hi donarà resposta ràpida fora de la planificació establerta.

3.14. Integració amb altres equips

L'adjudicatari del contracte basat haurà de portar a terme les activitats d'integració amb la resta d'equips operatius que conformen l'Agència, tant amb personal intern com amb personal d'altres empreses contractistes.

Aquesta integració s'haurà de portar a terme tant a nivell de la operativa diària (per garantir l'execució dels processos de la cadena de valor de l'Agència) com a nivell tàctic i operatiu.

Tot i això, els models de relació han de garantir els següents punts:

- Participació de l'adjudicatari en els processos que l'afectin.
- Compartició d'informació sobre fets puntuals (incidències, alertes, vulnerabilitats, etc.), ja sigui amb l'Agència com directament amb altres proveïdors.
- Compartició d'informació sobre fets agregats (tendències, patrons) i sobre afectacions col·lectives als diferents clients de l'Agència.
- Eliminació de les sitges organitzatives.
- Creació d'un fons comú de coneixement sobre la seguretat de la informació.

- Creació de bucles de retroalimentació que facilitin una resposta àgil davant de qualsevol nova situació en matèria de seguretat.

