

**Plec de prescripcions tècniques
particulars que regeix la contractació
basada en l'acord marc serveis
consultoria en sistemes i consultoria
tècnica per a la contractació del
servei de suport a la Unitat d'anàlisi
en ciberseguretat**

Exp. CB25AMCONSL1B007

Índex

1	Introducció	4
1.1	Funcions de l'Agència de Ciberseguretat de Catalunya rellevants a efectes del la nova estratègia de contractació	4
1.2	Context	5
1.2.1	Metodologia Ciber4i	5
1.2.2	Eines disponibles	5
2	Descripció dels serveis objecte de la contractació basada	7
2.1	Context dels serveis objecte de la licitació	7
2.2	Objecte i abast dels serveis	7
2.3	Objectius del servei	7
2.4	Característiques del servei	8
2.4.1	Organització del servei	8
2.4.2	Metodologia de treball	9
2.5	Qualitat dels lliurables	10
2.6	Criteris lingüístics i rigor comunicatiu dels lliurables	10
2.6.1	Millores	11
2.7	Activitats del servei	12
2.8	Lliurables del servei	13
2.8.1	Serveis no recurrents	15
3	Condicions d'execució del servei	17
3.1	Horaris	17
3.2	Localització física	17
3.3	Equip de treball	17
3.3.1	Perfils	18
3.4	Canvi de recurs	19
3.5	Control de rotació	20
3.6	Eines i equipament per a la prestació de serveis	20
3.7	Gestió del coneixement	21
3.8	Seguretat Corporativa	22
3.9	Control de Gestió	22
3.10	Documentació	23
3.11	Formació	23
3.12	Contingència	23
3.13	Metodologia, estàndards i lliurables	24
3.14	Seguretat	24
3.14.1	Deure de confidencialitat	24

3.14.2 Dades de caràcter personal.....	24
3.14.3 Compliment del marc legal de ciberseguretat i del marc normatiu intern	24
3.14.4 Capacitat tècnica	25
3.14.5 Adquisició de productes/eines i productes o serveis de seguretat	25
3.14.6 Interconnexions	26
3.14.7 Verificació del compliment i auditoria.....	26
3.14.8 Incidents de seguretat	26
3.14.9 Accés a la informació.....	26
3.15Assegurament i control de la qualitat i la millora contínua.....	26
3.16Seguiment del servei	27
3.17Integració amb altres equips.....	28

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. Dins d'aquest context, els acords marc en matèria de ciberseguretat representen una eina essencial per a la implementació de solucions i serveis que reforcin la ciberseguretat de Catalunya, alineats amb l'Estratègia de Ciberseguretat 2019-2022 i la proposta per a la nova Estratègia 2023-2027.

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 aquesta 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 nivell d'activitat de gestió de més de 4.424 milions de ciberatacs durant el 2022, una xifra 20 cops superiors a la del 2021.

D'aquests 4.424 milions de ciberatacs gestionats, 2.175 van esdevenir en un incident efectiu de seguretat gestionat per l'Agència de Ciberseguretat, el que representa una reducció del 22% respecte de l'any 2021.

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.

1.1 Funcions de l'Agència de Ciberseguretat de Catalunya rellevants a efectes de la nova estratègia de contractació

Avui en dia l'Agència té les següents funcions:

- L'Àrea de Gerència s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació i la gestió de personal.

- Operació de la Seguretat du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció, resposta i recuperació de seguretat en la seva vessant més operativa i la seguretat corporativa.
- Desenvolupament d'Estratègia d'Àmbits té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes i iniciatives de seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- Producte i Centres de Competència i Innovació (DIP) s'ocupa, per una banda, d'identificar les necessitats i proposar noves idees i estratègies per a l'elaboració de nous productes generats per l'Agència o millora dels existents, i coordina l'execució del cicle de vida dels productes, des de la seva concepció fins a la seva retirada, incloent el disseny, desenvolupament, desplegament i control de qualitat. Per una altra banda, coordina, cohesiona i capacita l'ecosistema de la Ciberseguretat de Catalunya, recolzant el coneixement, sensibilització i conscienciació com a palanca de la transformació i creixement del sector.
- Certificacions en matèria de Ciberseguretat per desplegar totes les eines i processos vinculats al procés de certificació en ciberseguretat de les entitats, garantint sempre la independència necessària per la correcta execució d'aquests processos.

1.2 Context

1.2.1 Metodologia Ciber4i

El Model Ciber4i és la metodologia pròpia de l'Agència per a la generació de productes analítics orientats a la presa de decisions en matèria de ciberseguretat. Es tracta d'un model de col·laboració que articula la relació entre l'Agència, l'Entorn Operatiu (d'on sorgeixen les amenaces) i la Comunitat de Ciberseguretat, amb l'objectiu d'alinejar les necessitats d'informació amb l'acció operativa i estratègica.

El model s'estructura al voltant de quatre processos interconnectats (4i):

- **Priorització** (*Intent*), mitjançant el qual s'estableixen les prioritats i necessitats d'informació consensuades amb la Comunitat de Ciberseguretat.
- **Interpretació** (*Interpret*), que consisteix en la recopilació i anàlisi sistemàtica de la informació provinent de l'Entorn Operatiu.
- **Orientació** (*Influence*), a través del qual l'Agència elabora productes analítics i recomanacions específiques de caràcter operatiu, tàctic o estratègic.
- **Impacte** (*Impact*), que correspon a la implementació de mesures per part de la Comunitat de Ciberseguretat per mitigar o contrarestar les amenaces identificades.

A mode simplificat, el Model Ciber4i es materialitza mitjançant el *Procés Analític*, que estructura la planificació, obtenció, anàlisi, producció i difusió de la informació de manera contínua i iterativa, garantint la coherència, traçabilitat i qualitat dels productes generats.

1.2.2 Eines disponibles

Per al desenvolupament de l'anàlisi de tendències, l'Agència disposa d'eines corporatives que donen suport a l'obtenció, seguiment i explotació d'informació en ciberseguretat, facilitant una anàlisi rigorosa i contextualitzada de les tendències amb impacte a Catalunya.

- a) **Eina de Tendències de Ciberseguretat.** L'Eina de Tendències és una plataforma d'anàlisi desenvolupada per l'Agència per tal de recopilar, classificar i analitzar notícies de ciberseguretat provinents de fonts RSS i entrades manuals. Inclou un cercador avançat,

gràfiques de correlació de termes, i indicadors PowerBI tant generals com específics de Catalunya, que faciliten la identificació de patrons, sectors afectats, vectors d'entrada i evolució temporal.

- b) **Feedly.** L'Agència disposa de llicència d'ús de l'eina Feedly, plataforma de monitorització i agregació de continguts digitals orientada al seguiment sistemàtic de fonts d'informació especialitzades. Aquesta eina permet centralitzar, organitzar i prioritzar informació procedent de mitjans especialitzats, blogs tècnics, publicacions institucionals, organismes internacionals, proveïdors tecnològics i altres fonts rellevants en matèria de ciberseguretat. Facilita la configuració de fluxos temàtics, la classificació per etiquetes i l'ús de filtres intel·ligents per detectar continguts d'interès, així com la identificació de tendències emergents.
- c) **Catàleg d'indicadors de l'Agència.** L'Agència disposa d'un catàleg corporatiu d'indicadors vinculats a la seva pròpia activitat en els diferents àmbits d'actuació. Aquest conjunt d'indicadors pot constituir una font de suport per a la Unitat d'anàlisi en aquells casos en què resultin representatius o aportin coneixement rellevant per a la interpretació de tendències en matèria de ciberseguretat a Catalunya. Els indicadors disponibles reflecteixen l'activitat, serveis i àmbits d'intervenció de l'Agència i, per tant, poden oferir una visió contextualitzada de determinades dinàmiques observades en l'entorn català.
- d) **Microsoft Loop.** Microsoft Loop és l'eina corporativa utilitzada per estructurar i compartir la informació del servei, actuant com a plataforma central de gestió del coneixement i dels fluxos analítics. Amb l'eina s'organitzen processos, documentació i components dinàmics en un entorn col·laboratiu, garantint la coherència i la traçabilitat. Un Loop és l'espai bàsic de treball de la Unitat d'Anàlisi; tanmateix, podrà ser substituït per una eina especialitzada alternativa si el Responsable del Servei ho considera necessari, sense cost addicional per a l'Agència.

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.01.2024 que regeix l'Acord Marc "Serveis de consultoria en sistemes i consultoria tècnica".

Concretament s'emmarca en el: Lot 1.

Dins de dit lot s'inclouen les actuacions d'un servei de suport a la Unitat d'anàlisi en ciberseguretat, les quals son plenament assimilables a l'objecte de la present licitació.

2.2 Objecte i abast dels serveis

L'objecte de la present licitació és la contractació d'un servei de suport a la Unitat d'anàlisi en ciberseguretat, mitjançant serveis especialitzats d'anàlisi, interpretació i generació de coneixement sobre l'estat i l'evolució de la ciberseguretat, amb una perspectiva estratègica, sectorial i territorial de Catalunya, amb la finalitat de donar suport a les funcions i a la presa de decisions seguint les directrius de l'Agència.

En concret, el present contracte basat inclou, entre d'altres, l'anàlisi continuada d'informació rellevant procedent de fonts internes i externes especialitzades, la identificació de tendències, riscos, oportunitats i escenaris futurs, així com l'elaboració de productes analítics, executius i de difusió pública, com ara informes de tendències i prospectiva, estudis sectorials, resums executius i documents analítics diversos per donar resposta a les necessitats de l'Agència.

Totes les prestacions objecte del contracte s'han de dur a terme en coordinació amb tots els serveis de l'Agència, i s'hauran d'ajustar als requeriments, plantilles i metodologia analítica pròpia de l'Agència, garantint la coherència, homogeneïtat i qualitat dels productes analítics elaborats.

2.3 Objectius del servei

- Realitzar un anàlisi continuat i sistemàtic de la informació rellevant en matèria de ciberseguretat, procedent de fonts pròpies de l'Agència i de fonts externes especialitzades, garantint-ne la qualitat, rellevància i actualització.
- Identificar tendències emergents, riscos, oportunitats i possibles escenaris futurs, amb una perspectiva estratègica, sectorial i territorial, que permeti anticipar l'impacte de l'evolució de la ciberseguretat en els diferents àmbits d'interès de l'Agència.
- Generar intel·ligència analítica d'alt valor afegit, mitjançant l'elaboració de productes estructurats (informes, resums executius, estudis sectorials, prospectives i altres lliurables), adaptats als diferents destinataris i alineats amb la metodologia analítica pròpia de l'Agència.
- Donar suport transversal a les diferents àrees i serveis de l'Agència, mitjançant l'aportació de coneixement expert i anàlisi especialitzada que contribueixi a la presa de decisions operatives, tàctiques i estratègiques.
- Contribuir al posicionament institucional de l'Agència com a referent en l'àmbit de l'anàlisi i la prospectiva en ciberseguretat, mitjançant la generació de continguts rigorosos, estructurats i de qualitat.

2.4 Característiques del servei.

El servei de suport a la Unitat d'Anàlisi en ciberseguretat ha de configurar-se com una capacitat estable, especialitzada i altament professionalitzada d'anàlisi integral de la ciberseguretat, orientada a la generació de coneixement expert, prospectiu i accionable, d'acord amb la metodologia analítica i els requeriments establerts per l'Agència.

Les característiques essencials del servei són les següents:

2.4.1 Organització del servei

El servei de suport a la Unitat d'anàlisi en ciberseguretat haurà de disposar d'una organització estable, especialitzada i flexible que garanteixi la correcta execució de les prestacions al llarg de tota la durada del contracte. Aquesta organització haurà de permetre donar resposta a les necessitats de l'Agència en matèria d'anàlisi integral de la ciberseguretat, assegurant la continuïtat del servei, la seva coherència metodològica i la seva adaptació a possibles variacions en la càrrega de treball o a noves prioritats estratègiques.

El servei haurà d'estar estructurat de manera que cobreixi de forma completa totes les fases del cicle analític, amb una definició clara de rols i responsabilitats. Així mateix, haurà de facilitar la coordinació efectiva amb les diferents àrees, serveis i col·laboradors de l'Agència per tal de garantir la coherència dels productes elaborats i la integració de coneixement transversal. Igualment, l'organització haurà de preveure mecanismes que permetin gestionar situacions imprevistes, desviacions respecte a la planificació inicial o necessitats sobrevingudes, assegurant en tot moment la qualitat i eficiència del servei.

L'organització del servei haurà d'incorporar perfils per nodrir dues vessants funcionals complementàries, que actuaran de manera coordinada i no seqüencial: una vessant tècnica, orientada al coneixement especialitzat en ciberseguretat i al desenvolupament analític, i una vessant discursiva, orientada a garantir la claredat, comprensió i adequació formal dels productes generats. Ambdues vessants formen part del mateix procés i contribuiran conjuntament a l'elaboració dels lliurables, sense compartiments funcionals ni fases exclusives.

Vessant tècnica

Aquesta vessant concentra la capacitat d'anàlisi especialitzada, la interpretació del context de ciberseguretat i la formulació de conclusions fonamentades. Inclou el domini del panorama de ciberamenaces, tecnologies, vectors emergents i fonts d'informació especialitzades, així com la capacitat de garantir el rigor i la coherència metodològica del procés analític.

Aptituds vinculades a la vessant tècnica:

- Capacitat analítica avançada i criteri expert en ciberseguretat.
- Domini d'eines i metodologies d'obtenció i explotació d'informació.
- Capacitat de contextualitzar la informació i identificar tendències rellevants.
- Capacitat de formular conclusions i recomanacions fonamentades.

Vessant discursiva

Aquesta vessant assegura que els continguts analítics es presenten de manera clara, estructurada i adaptada als diferents destinataris. Inclou la redacció, síntesi, adequació lingüística i elaboració de materials que facilitin tant la comprensió interna com la difusió pública, d'acord amb les guies de comunicació clara, llenguatge inclusiu i no sexista.

Aptituds vinculades a la vessant discursiva:

- Capacitat acreditada de redacció, síntesi i estructuració de continguts complexos.
- Capacitat analítica i coneixements en ciberseguretat.
- Domini d'eines i metodologies d'obtenció i explotació d'informació.
- Competència en comunicació clara i adaptació del discurs a diferents destinataris.
- Domini de guies de llenguatge inclusiu, llenguatge no sexista i criteris formals exigits.
- Capacitat de traduir contingut especialitzat en formats comprensibles i d'alt impacte.

Les dues vessants hauran d'actuar de manera integrada, amb interacció continuada en totes les fases del procés analític. Cap vessant no quedarà restringida a una fase concreta, sinó que totes dues hauran de:

- contribuir simultàniament a la definició d'enfocs i criteris de treball;
- participar en la revisió i validació dels continguts;
- garantir que els productes resultants combinen rigor tècnic i claredat comunicativa;
- adaptar-se a les necessitats específiques de cada tipus de producte i destinatari.

L'adjudicatari haurà d'assegurar que l'equip presenta una configuració que integri les dues vessants de manera funcional i equilibrada, amb perfils que permetin cobrir amb garanties tant el coneixement tècnic com la capacitat de comunicació i divulgació. La proposta haurà d'explicitar com s'articulen aquestes dues vessants dins l'organització del servei.

2.4.2 Metodologia de treball

La prestació del servei s'haurà de dur a terme seguint una metodologia de treball estructurada, sistemàtica i alineada amb el model analític propi de l'Agència, que permeti planificar, executar i controlar les diferents activitats de manera estructurada i documentada. Aquesta metodologia haurà d'estar adaptada al caràcter estratègic i continuat de l'anàlisi de la ciberseguretat i haurà de permetre l'obtenció de coneixement expert sobre l'estat actual i els escenaris futurs.

El servei haurà d'incloure procediments sistemàtics per a la identificació i selecció de fonts d'informació rellevants, el tractament rigorós de la informació disponible, l'elaboració d'anàlisis contextualitzades i la producció de lliurables adaptats als diferents destinataris. Igualment, haurà d'incorporar mecanismes de seguiment i revisió periòdica de l'activitat analítica, així com processos de recollida de valoracions que permetin la millora contínua del servei i l'adequació dels productes a les necessitats reals de l'Agència.

La metodologia de treball haurà d'incorporar de manera explícita la participació coordinada de les dues vessants funcionals definides al servei: la vessant tècnica i la vessant discursiva. Ambdues vessants hauran d'interactuar de forma continuada al llarg de totes les fases del procés analític, sense compartiments funcionals ni seqüenciacions estrictes, assegurant que:

- la vessant tècnica aporta els elements d'anàlisi, interpretació i validació necessaris per fonamentar el coneixement generat;
- la vessant discursiva estructura, sintetitza i formalitza els continguts perquè siguin clars, coherents i adequats als diferents tipus de productes i destinataris.

L'adjudicatari haurà d'establir els mecanismes interns de coordinació que permetin integrar les aportacions de totes dues vessants de manera simultània i traçable en els procediments de planificació, revisió i producció dels diferents lliurables.

2.5 Qualitat dels lliurables

El servei haurà de garantir que tots els productes elaborats compleixin uns estàndards elevats de qualitat analítica, formal i lingüística. Els lliurables hauran d'estar degudament estructurats, argumentats i contextualitzats, amb conclusions fonamentades i coherents amb les evidències analitzades.

El servei haurà d'incloure processos interns de revisió i validació prèvia al lliurament, orientats a assegurar el rigor analític, la consistència dels continguts i la correcció ortogràfica. Els documents elaborats hauran de presentar una redacció clara, precisa i comprensible, amb una estructura ordenada, un llenguatge adequat als diferents públics destinataris i un ús correcte de la terminologia pròpia de la ciberseguretat. En aquells documents destinats a publicació oberta, s'hauran de preveure mecanismes específics de revisió lingüística i ortogràfica qualificada que garanteixin la correcció gramatical, ortotipogràfica i estilística abans del lliurament definitiu.

A més, tots els lliurables elaborats en el marc del servei hauran de complir els criteris d'accessibilitat establerts per les *Web Content Accessibility Guidelines (WCAG)* en la seva versió 2.2, publicades pel W3C com a recomanació oficial. Aquestes directrius inclouen requisits orientats a garantir una millor experiència per a persones amb discapacitats visuals, cognitives, motores i per a l'ús en dispositius mòbils i esdevenen l'estàndard de referència per assegurar que els continguts siguin perceptibles, operables, comprensibles i robustos per a tota la ciutadania. En conseqüència, els documents del servei hauran de seguir els criteris de conformitat corresponents, especialment els de nivell AA, reconeguts internacionalment com el nivell recomanat per garantir l'accessibilitat digital.

La guia pot trobar-se a aquest enllaç: <https://www.w3.org/TR/WCAG2>

2.6 Criteris lingüístics i rigor comunicatiu dels lliurables

Per garantir que els informes, anàlisis i productes de coneixement generats compleixin els estàndards de rigor, inclusió i claredat, tots els lliurables del servei hauran de seguir les indicacions establertes per la Generalitat de Catalunya en matèria de comunicació clara, llenguatge inclusiu i ús no sexista de la llengua a través de les guies específiques que es detallen a continuació. Aquests criteris seran objecte de revisió en cada lliurament i la seva adequació serà requerida com a condició d'acceptació dels productes.

Comunicació Clara

Els productes que generi el servei hauran d'ajustar-se als criteris de comunicació clara establerts per la Generalitat de Catalunya, d'acord amb les directrius definides a la "*Guia de comunicació clara*". A aquest efecte, s'haurà de garantir, com a criteris verificables que, a tots els productes analítics:

- El text utilitza llenguatge planer i evita tecnicismes innecessaris, redundàncies i formulacions confuses;
- L'estructura presenta una jerarquia clara d'informació, amb títols i subtítols entenedors i paràgrafs curts;
- L'organització del contingut facilita la lectura mitjançant llistes, destacats o altres recursos de claredat;
- El disseny del document assegura la llegibilitat, incloent-hi tipografia adequada, contrast suficient i ús correcte de l'espai en blanc; i
- Tots els continguts compleixen els requisits d'accessibilitat i inclusió que la Guia estableix per garantir la comprensió per part de qualsevol perfil destinatari.

Enllaç a la “Guia de comunicació clara”: https://atenciociutadana.gencat.cat/web/.content/0-subweb-comunicacio-clara/home/destacat-guia-pdf/guia_de_comunicacio_clara.pdf

Llenguatge no sexista

Els productes que generi el servei hauran d'ajustar-se als criteris d'ús no sexista de la llengua establerts per la Generalitat de Catalunya, d'acord amb la “*Guia d'usos no sexistes de la llengua*”. A aquest efecte, s'haurà de garantir que els productes:

- Facin ús de formes genèriques adequades i mots col·lectius quan sigui possible;
- Substitueixin del masculí com a genèric mitjançant alternatives basades en l'acció, la funció o l'organisme;
- Tinguin preferència per expressions despersonalitzades que evitin atribucions de gènere;
- Facin ús justificat i moderat de formes dobles; i
- Facin servir recursos lingüístics neutres en adjectius, perífrasis i altres elements susceptibles de marcar gènere.

Enllaç a la “Guia d'usos no sexistes de la llengua”

<https://llengua.gencat.cat/web/.content/documents/publicacions/altres/arxius/guiausosnosexistes.pdf>

Llenguatge inclusiu

Els productes que generi el servei hauran de complir els criteris de llenguatge inclusiu establerts per la Generalitat de Catalunya, d'acord amb el que disposa la “*Guia de llenguatge inclusiu*”. A aquest efecte, s'haurà de garantir, de manera verificable, que:

- S'hi prioritza sempre la persona per damunt de qualsevol condició o discapacitat;
- No s'hi utilitza terminologia obsoleta, pejorativa o estigmatitzadora;
- Només es fa referència a la discapacitat quan és rellevant per al contingut;
- S'hi emprava terminologia adequada i inclusiva, d'acord amb les formes recomanades per la Direcció General de Política Lingüística;
- Els textos presenten una imatge rigorosa, no estereotipada i respectuosa de les persones.

Enllaç a la “Guia de llenguatge inclusiu”:

https://llengua.gencat.cat/web/.content/documents/publicacions/publicacions_en_linia/arxius/guia-llenguatge-inclusiu.pdf

2.6.1 Millores

El servei haurà d'estar orientat a la millora contínua i a l'enriquiment progressiu de les capacitats analítiques de la Unitat d'Anàlisi. En aquest sentit, es fomentarà la incorporació de noves fonts d'informació que permetin ampliar la base de coneixement disponible i millorar la contextualització de les anàlisis, així com la introducció de tècniques o eines de suport que contribueixin a optimitzar els processos d'anàlisi i producció de coneixement.

Qualsevol proposta d'automatització o ús de tecnologies emergents haurà d'estar orientada a reforçar el procés analític i a millorar l'eficiència del servei, sense substituir en cap cas el criteri expert ni la validació humana dels continguts elaborats. Igualment, es valorarà la proposta de nous formats

o enfocaments que permetin incrementar la claredat, utilitat i impacte dels productes generats per la Unitat d'Anàlisi.

2.7 Activitats del servei

L'activitat del servei de suport a la Unitat d'Anàlisi en ciberseguretat tindrà com a finalitat la generació sistemàtica de coneixement expert sobre l'estat, l'evolució i els possibles escenaris futurs de la ciberseguretat, amb una perspectiva estratègica, sectorial i territorial alineada amb les funcions i necessitats de l'Agència. El servei haurà de configurar-se com un centre de coneixement especialitzat, capaç d'integrar informació procedent de diverses fonts, interpretar-la amb criteris de rigor analític i transformar-la en productes estructurats, útils i orientats a la presa de decisions.

Aquesta activitat haurà d'anar més enllà de la mera recopilació d'informació, incorporant processos d'anàlisi, contrast, contextualització i síntesi que permetin identificar tendències, riscos, oportunitats i dinàmiques emergents en l'àmbit de la ciberseguretat. El servei haurà de disposar de capacitats expertes per interpretar fenòmens complexos, formular hipòtesis, valorar evidències i elaborar conclusions fonamentades que aportin valor estratègic a l'Agència.

El servei de suport a la Unitat d'anàlisi haurà d'actuar com a punt de referència intern en matèria de coneixement especialitzat en ciberseguretat, contribuint de manera transversal a les diferents àrees i serveis de l'Agència i generant productes analítics adaptats als diversos públics destinataris, d'acord amb els requeriments i la metodologia establerts per l'Agència.

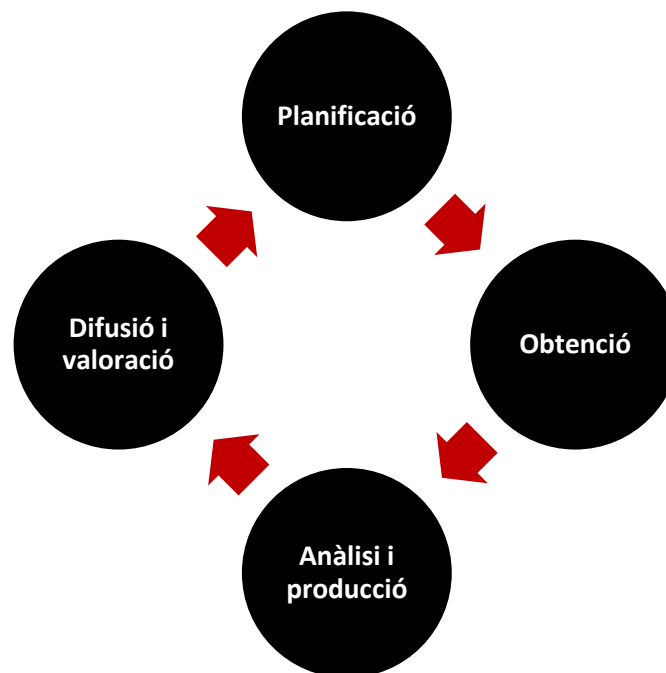


Diagrama del Cicle Analític de la Unitat d'anàlisi

L'activitat del servei de suport a la Unitat d'anàlisi es pot explicar de forma simplificada amb un *Cicle Analític*, concebut com un procés continu i iteratiu que garanteixi la coherència, traçabilitat i qualitat del coneixement generat. Aquest cicle comprèn les fases de planificació, obtenció, anàlisi i producció, i difusió i feedback, les quals es desenvoluparan de manera coordinada i alineada amb les directrius establertes per l'Agència.

1) Planificació

L'Agència establirà les directrius de cada producte analític.

2) Obtenció

- a) Identificar fonts d'informació que aportin mètriques en matèria de ciberseguretat.
- b) Mantenir actualitzat el conjunt de fonts d'informació disponibles.
- c) Avaluar i filtrar la idoneïtat de les fonts per evitar el col·lapse per excés.
- d) Recol·lectar informació en brut de diferents fonts i per diferents mitjans.
- e) Convertir la informació recol·lectada en bases de dades estructurades i explotables.
- f) Assegurar especialment que s'obté la informació

3) Anàlisi i producció

- a) Extreure coneixement induït de pautes i relacions entre les dades (*data mining*).
- b) Valorar la credibilitat, oportunitat i exactitud de la informació obtinguda i processada en termes de pertinència, coherència, utilitat i rellevància.
- c) Aportar capacitats intel·lectuals i coneixement per tal de dotar la informació de sentit i comprensibilitat amb l'objectiu que el destinatari pertinent pugui entendre i utilitzar-la.
- d) Identificar les principals amenaces de ciberseguretat que poden tenir impacte en els diferents àmbits de la societat digital.
- e) Elaborar la tipologia documental adequada per presentar el resultat del procés: informes, resums, dossiers, esquemes, presentacions, conceptualització d'infografies, etc.
- f) Adequar els diferents tipus de documents als criteris de comunicació clara, llenguatge no sexista i llenguatge inclusiu d'acord amb les guies específiques de la Generalitat de Catalunya.
- g) Realitzar la correcció ortogràfica formal en el cas de productes destinats a publicar-se en obert i assegurar-ne el compliment amb les recomanacions d'accessibilitat dels documents.
- h) Assegurar un enfocament particular i un interès específic segons la realitat de Catalunya.

4) Difusió i Valoració

- a) Distribuir i posar els productes generats a disposició dels destinataris que escaigui en cada cas.
- b) Promoure l'obtenció d'impacte a partir de la difusió dels productes elaborats.
- c) A partir de les conclusions obtingudes en el desenvolupament de la funció analítica, efectuar correccions per a la seva millora contínua i proposar noves iniciatives.
- d) Endegar accions, com enquestes valoratives, per tal de comprendre el consumidor amb l'objectiu de millorar els productes elaborats.

2.8 Lliurables del servei

Tots els lliurables elaborats en el marc del present contracte hauran de constituir productes analítics propis, originals i específicament adaptats a la realitat de Catalunya. Hauran de copsar la realitat de

la ciberseguretat amb afectació o interès per a Catalunya, integrant el context internacional amb l'anàlisi de l'impacte local, els sectors implicats i les implicacions estratègiques per a l'Agència.

El servei no té per objectiu reproduir o sintetitzar continguts ja existents en l'àmbit global de la ciberseguretat, sinó interpretar i analitzar les tendències, dinàmiques i esdeveniments rellevants des d'una perspectiva territorial, sectorial i institucional pròpia. Prioritàriament, hauran de tenir en compte els fets rellevants ocorreguts a Catalunya i incorporar indicadors propis de l'Agència o de terceres fonts amb implicació directa en l'àmbit català, sens perjudici que, en determinats casos, es puguin utilitzar indicadors procedents de fonts externes quan aquests resultin representatius i aportin valor a l'anàlisi.

- 5) **Resums de tendències mensuals.** Elaboració de resums de tendències mensuals que hauran de recollir les 3 principals tendències identificades en matèria de ciberseguretat durant el període de referència, així com els fets rellevants i indicadors que donin suport i justifiquin l'anàlisi realitzat. Els documents hauran de tenir un format executiu, clar i orientat a facilitar la comprensió i la presa de decisions.
 - a) Volumetria: onze (11) resums de tendències per any natural, atès que els mesos de juliol i agost es presentaran en un únic informe.
 - b) Data de lliurament: primera quinzena de cada mes.
 - c) Difusió: pública.
 - d) Exemple: <https://ciberseguretat.gencat.cat/ca/dades-ciberseguretat/tendencies-ciberseguretat/resum-tendencies-mensuals-ciberseguretat/>
- 6) **Informe anual de tendències.** Elaboració d'un informe anual, a presentar a l'inici de cada any natural, que analitzi de manera estructurada les principals dinàmiques observades durant l'any anterior. Aquest informe haurà d'incloure la contextualització dels fenòmens més rellevants, l'anàlisi de la seva evolució, la identificació de sectors potencialment afectats i les implicacions estratègiques per a l'Agència. Addicionalment, inclourà els fets rellevants i indicadors que donin suport i justifiquin l'anàlisi realitzat.
 - a) Volumetria: un (1) informe anual.
 - b) Data de lliurament: primers dos mesos de l'any.
 - c) Difusió: pública.
 - d) Exemple: <https://ciberseguretat.gencat.cat/ca/dades-ciberseguretat/tendencies-ciberseguretat/resum-tendencies-mensuals-ciberseguretat/>
- 7) **Informe anual de perspectives.** Elaboració d'un informe anual, a presentar al final de cada any natural, orientat a identificar i descriure els possibles escenaris futurs en matèria de ciberseguretat per al període següent. El document haurà d'incloure l'anàlisi de tendències emergents, riscos previsibles, tecnologies rellevants i oportunitats potencials, així com una valoració argumentada de la seva possible evolució.
 - a) Volumetria: un (1) informe anual.
 - b) Data de lliurament: mitjan desembre.
 - c) Difusió: pública.
 - d) Exemple: <https://ciberseguretat.gencat.cat/ca/dades-ciberseguretat/tendencies-ciberseguretat/prospectives/>
- 8) **Informe "La ciberseguretat a Catalunya".** Elaboració anual d'un informe conjunt amb ACCIÓ (l'Agència per a la competitivitat de l'empresa de la Generalitat de Catalunya) orientat a oferir una

visió integrada de l'estat de la ciberseguretat a Catalunya. L'informe combinarà l'anàlisi de l'ecosistema empresarial i la dinamització del sector, aportada per ACCIÓ, amb l'expertesa tècnica en ciberseguretat del servei de suport a la Unitat d'Anàlisi. Inclourà la recopilació i interpretació d'informació rellevant sobre l'activitat en ciberseguretat a Catalunya i els principals esdeveniments i tendències internacionals amb afectació local, així com la definició d'un missatge coherent i unificat alineat amb els objectius institucionals.

- a) Volumetria: un (1) informe anual.
- b) Data de lliurament: un mes abans de la data de celebració del Barcelona Cybersecurity Congress.
- c) Difusió: pública.
- d) Exemple: https://ciberseguretat.gencat.cat/web/.content/06_dadesCiberseguretat/altres-informes-ciberseguretat/Ciberseguretat-a-Catalunya-2025_informe-tecnologic.pdf

9) Suport analític a peticions internes. Prestació de suport puntual a les diferents àrees i serveis de l'Agència mitjançant l'elaboració d'argumentaris per a comunicació institucional, reculls de dades i informació per a campanyes o iniciatives específiques, així com l'anàlisi i documentació de qüestions sobrevingudes en els diferents àmbits d'actuació de l'Agència. Aquest suport haurà de proporcionar-se amb diligència i amb el mateix nivell d'exigència analítica i formal que la resta de lliurables.

- a) Volumetria: sota demanda.
- b) Data de lliurament: sota demanda.
- c) Difusió: interna.

10) Recull de neologismes en ciberseguretat. Identificació, recopilació i proposta anual de nova terminologia emergent en l'àmbit de la ciberseguretat, amb especial atenció als termes d'ús recent o procedents d'altres idiomes que puguin requerir adaptació o normalització en català. El servei haurà d'elaborar un recull estructurat de termes amb la corresponent definició i contextualització, amb l'objectiu de treballar-los conjuntament amb el Termcat per a la seva eventual validació i publicació al diccionari terminològic de ciberseguretat.

- a) Volumetria: 20-30 termes anuals.
- b) Data de lliurament: anualment.
- c) Difusió: interna.
- d) Exemple: <https://www.termcat.cat/ca/diccionaris-en-linia/239>

11) Documentació del servei. Elaboració i manteniment de la documentació associada a l'activitat del servei de suport a la Unitat d'anàlisi, incloent la planificació anual de treball, els criteris metodològics aplicats, el registre de fonts utilitzades i qualsevol altra documentació necessària per garantir la traçabilitat, coherència i continuïtat del servei.

2.8.1 Serveis no recurrents

Adicionalment als serveis recurrents, l'Agència també necessita suport en actuacions puntuals o extraordinàries que excedeixin els lliurables recurrents previstos en el contracte i responguin a noves necessitats analítiques, normatives o estratègiques en el sector de la Salut que, per la seva naturalesa, no puguin ser considerades recurrents. Aquests serveis es consideraran com a no recurrents.

L'Agència estableix la possibilitat de dur a terme projectes o prestacions de serveis de caràcter no recurrent, vinculats a necessitats sobrevingudes d'ampliació d'abast analític, adaptacions

normatives o estratègiques, o suport analític extraordinari en l'àmbit de la Salut. la volumetria dels quals no es pot preveure ni concretar en el moment d'elaborar aquest plec, atesa la seva dependència de factors externs o estratègics.

Aquesta prestació no recurrent es durà a terme a criteri de l'Agència en funció de les necessitats en cada cas. Aquestes prestacions dependran de que, si s'escau, es rebi la petició per a dur a terme la prestació de serveis, que es disposi de la partida econòmica necessària per a dur a terme l'execució d'aquests projectes i de que l'empresa licitadora ofereixi una solució competitiva en el moment en que se sol·liciti la seva execució.

La gestió dels serveis no recurrents es durà a terme mitjançant ordres de treball específiques degudament autoritzades per l'Agència, en les quals es definirà l'abast, la durada, els lliurables i el pressupost associat a cada actuació.

Com a exemples de serveis o projectes que es poden sol·licitar en aquest nivell de prestació, sense ser excloents, són els següents:

- Elaboració d'informes de tendències sectorials per a l'àmbit Salut, amb periodicitat trimestral (un a lliurar el primer mes després de cada trimestre vençut: gener, abril, juliol i octubre), seguint el model dels resums mensuals de tendències.
- Suport analític intensiu en situacions excepcionals en l'àmbit de la Salut, com incidents greus de ciberseguretat, campanyes d'amenaça amb impacte rellevant o esdeveniments que requereixin una anàlisi específica i urgent.

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 podria demanar la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

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 en la ubicació dels professionals, 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 (descriuint-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 de les següents figures que conjuntament assumiran les tasques del servei. A aquest efecte, cadascun ha de assumir les següents responsabilitats:

Perfil	Responsabilitats principals atribuïdes
Consultor en Ciberseguretat 1	Realitzarà les tasques o informes que li siguin encomanats, dintre dels marges de qualitat, temps i cost establerts. Aquest perfil serà responsable del reporting periòdic de l'evolució i resultats del servei i assegurar la informació regular a l'Agència segons els terminis marcats.
Consultor en Ciberseguretat 2	Realitzarà les tasques o informes que li siguin encomanats, dintre dels marges de qualitat, temps i cost establerts.

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 recurrents demanats en aquest plec és de 1.299,83 hores per l'any 2026 i 2.253,03 hores per a l'any 2027. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	% dedicació	Hores 2026	Hores 2027
Consultor en Ciberseguretat 1	70%	909,88	1.577,12
Consultor en Ciberseguretat 2	30%	389,9	675,91
	100%	1.299,83	2.253,03

Les dedicacions de la taula s'han d'entendre com a aproximades,.

3.3.1 Perfils

Els perfils de Consultor en Ciberseguretat hauran de reunir les característiques següents:

- Seleccionar, contrastar i interpretar informació rellevant amb criteris de rigor i coherència.
- Identificar tendències, riscos, oportunitats i escenaris en l'àmbit de la ciberseguretat amb afectació a Catalunya.
- Contextualitzar la informació en l'entorn català i en els àmbits d'interès de l'Agència.
- Formular conclusions i recomanacions fonamentades, d'acord amb la metodologia analítica establerta.

- El perfil de Consultor/a en Ciberseguretat inclou dues vessants funcionals complementàries, que poden ser exercides per persones diferents adscrites al mateix perfil:
 - vessant tècnica: analitzar, valorar i correlacionar informació especialitzada, aplicar criteri expert i impulsar el desenvolupament analític del servei;
 - vessant discursiva: redactar, sintetitzar i estructurar continguts de manera clara, aplicar criteris de comunicació clara, llenguatge inclusiu i no sexista, i adaptar els productes als diferents destinataris.
- Elaborar documents estructurats, clars i orientats a la presa de decisions, ajustant el nivell de tècnica segons el producte i el destinatari.
- Aplicar els criteris de qualitat formal, inclusió lingüística i rigor comunicatiu establerts per la Generalitat.
- Participar en processos de revisió interna per garantir que els productes combinen coherència analítica i claredat comunicativa.
- Cooperar amb la resta de membres del servei, integrant de manera simultània aportacions de les diferents vessants funcionals.
- L'adjudicatari haurà d'assegurar que el conjunt de persones adscrites al perfil de Consultor/a en Ciberseguretat cobreix globalment les dues vessants funcionals (tècnica i comunicativa), sense exigir que cada persona individual assumeixi totes les aptituds descrites.

Els requeriments mínims en termes d'experiència dels perfils professionals que poden compondre l'equip per als serveis recurrents són els següents:

Perfil	Requisits
"Consultor en Ciberseguretat 1" i "Consultor en ciberseguretat 2"	Formació acadèmica Un dels perfils ha de disposar d'un grau superior (FP) en ciberseguretat o titulació universitària relacionada a una disciplina TIC. L'altre perfil ha de disposar de titulació universitària. Experiència mínima Com a mínim, un dels perfils ha de disposar de 2 anys d'experiència mínima en projectes relacionats amb la ciberseguretat. L'altre perfil ha de disposar de 2 anys d'experiència mínima en projectes relacionats amb la ciberseguretat o amb la generació de contingut discursiu.

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 (CIC) 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 CIC.

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 com el personal de 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 proporcioni per tal efecte

3.11 Formació

El personal de l'empresa adjudicatària del contracte basat realitzarà, si s'escau, 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

Els licitadors 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:

3.14.1 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.

3.14.2 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.

3.14.3 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.

3.14.4 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.

3.14.5 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 Catàleg 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.

3.14.6 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.

3.14.7 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 a 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.

3.14.8 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.

3.14.9 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.

3.15 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.

3.16 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.

3.17 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.

