Plec de prescripcions tècniques particulars que regeix la contractació basada en l'acord marc serveis consultoría en sistemes i consultoría técnica per a un servei de dades i analítica avançada en l'àmbit de la salut

Exp. CB25AMCONSL2B002

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 Organització 5

1.2.2 Infraestructura tecnològica existent 6

1.2.3 Aplicacions existents 7

2 Descripció dels serveis objecte de la contractació basada 10

2.1 Context dels serveis objecte de la licitació 10

2.2 Objecte i abast dels serveis 10

2.3 Objectius del servei 10

2.4 Característiques del servei. 11

2.4.1 Organització del servei 11

2.4.2 Metodologia de treball 11

2.4.3 Solució tècnica 11

2.5 Activitats del servei 12

2.6 Lliurables del servei 13

3 Condicions d'execució del servei 15

3.1 Horaris 15

3.2 Localització física. 15

3.3 Equip de treball 15

3.3.1 Perfils 17

3.4 Canvi de recurs 17

3.5 Control de rotació 17

3.6 Eines i equipament per a la prestació de serveis. 18

3.7 Gestió del coneixement 19

3.8 Seguretat Corporativa 19

3.9 Control de Gestió 20

3.10 Documentació. 21

3.11 Formació 21

3.12 Contingència 21

3.13 Metodologia, estàndards i lliurables 21

3.14 Seguretat 22

3.14.1 Deure de confidencialitat 22

3.14.2 Dades de caràcter personal 22

3.14.3 Compliment del marc legal de ciberseguretat i del marc normatiu intern 22

3.14.4 Capacitat tècnica 23
3.14.5 Adquisició de productes/eines i productes o serveis de seguretat 23
3.14.6 Interconnexions 23
3.14.7 Verificació del compliment i auditoria 24
3.14.8 Incidents de seguretat 24
3.14.9 Accés a la informació 24
3.15 Assegurament i control de la qualitat i la millora contínua 24
3.16 Seguiment del servei 25
3.17 Integració amb altres equips 26

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 confiable 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 del 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.
- Àrea d'Innovació i Producte s'ocupa 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.
- Centre de Competència i Innovació en Ciberseguretat (CCI) s'ocupa de la coordinació, cohesió i capacitat de l'ecosistema de Cibeseguretat de Catalunya, recolza el coneixement, sensibilització i conscienciació, i la innovació com a palanca de transformació i creixement del sector i fomenta la captació de forns i la internacionalització de l'entitat.
- 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 Organització

Qualsevol actuació vinculada a nous desenvolupaments cal realitzar-se en coordinació amb les unitats corporatives de l'Agència implicades en la prestació del servei, en particular la Unitat de Ciència i Analítica de Dades, la Unitat de Mitjans Tècnics i la Unitat de Seguretat Corporativa, respectant els seus criteris, directrius i àmbits de responsabilitat.

- Unitat de Ciència i Analítica de dades

La Unitat de Ciència i Analítica de Dades (CAD) part de l' Àrea d'Innovació i Producte i és responsable de garantir una gestió integral, coherent i segura de les dades, assegurant que esdevinguin un actiu útil per a la presa de decisions i la governança de la ciberseguretat. La seva funció central és el Govern de la Dada: defineix el model organitzatiu i els estàndards comuns, estableix rols i responsabilitats, crea i manté taules mestres i un catàleg oficial d'indicadors, fixa polítiques d'accés i control i garanteix la qualitat, la traçabilitat i la unicitat de la informació. També assegura el compliment normatiu, la protecció de dades personals i l'ús segur i ètic de la informació i dels models d'intel·ligència artificial.

A partir d'aquest marc, la Unitat dissenya i manté l'arquitectura tècnica que permet centralitzar i integrar dades de múltiples sistemes, automatitzar-ne la ingesta i transformació i garantir-ne la interoperabilitat. Desenvolupa capacitats d'anàlisi avançada i modelització per detectar patrons, classificar riscos i generar informació accionable, alhora que incorpora automatismes i solucions d'IA per escalar processos i reduir càrrega manual. Complementàriament, analitza tendències i elabora informes periòdics que donen suport a la planificació estratègica i a la supervisió del nivell de ciberseguretat.

- Unitat de Mitjans Tècnics

La Unitat de Mitjans Tècnics és responsable de la gestió, manteniment i evolució de la infraestructura tecnològica de l'Agència, incloent els entorns *cloud*, les xarxes de comunicacions i els dispositius corporatius. Aquesta unitat garanteix la disponibilitat, estabilitat i rendiment dels sistemes, així com

la correcta configuració i operació de les plataformes tecnològiques sobre les quals es despleguen les solucions i serveis.

En aquest sentit, defineix i opera els entorns d'execució, gestiona els accessos i recursos d'infraestructura, i estableix els criteris tècnics per al desplegament, monitorització i operació dels sistemes, assegurant l'alineament amb els estàndards tecnològics corporatius.

- Unitat de Seguretat Corporativa

La Unitat de Seguretat Corporativa és responsable de definir, implantar i supervisar el marc de seguretat de la informació de l'Agència, garantint el compliment de la normativa aplicable i de les polítiques internes en matèria de ciberseguretat.

Aquesta unitat estableix les directrius, controls i procediments de seguretat que han de complir tots els sistemes i serveis, i participa en els processos de validació i autorització dels desplegaments en entorns productius. Així mateix, vetlla pel compliment del marc normatiu vigent (incloent ENS i normativa de protecció de dades), supervisa la gestió de riscos i coordina les actuacions relacionades amb la seguretat dels sistemes d'informació.

1.2.2 Infraestructura tecnològica existent

L'Agència opera en un entorn tecnològic basat en serveis del núvol i eines de l'ecosistema Microsoft, que donen suport al desplegament d'aplicacions, l'automatització de processos, la gestió de dades i l'anàlisi d'informació. Aquest entorn està estructurat en diferents capes de serveis que permeten la integració funcional entre aplicacions, dades i components d'IA.

- Infraestructura i gestió de dades
    - Microsoft Azure: plataforma de serveis al núvol que proporciona recursos d'infraestructura com màquines virtuals, emmagatzematge, bases de dades i serveis de xarxa, amb capacitat d'escalabilitat i gestió centralitzada.
    - Microsoft 365 E5: model de llicenciament que dona accés a aplicacions de productivitat (com Word, Excel, Teams), eines de col·laboració, serveis de seguretat avançada i gestió de la informació.
    - Microsoft Fabric: plataforma de dades que integra serveis per a la ingesta, transformació, governança i consulta de dades procedents de diverses fonts, facilitant-ne l'anàlisi unificada i en temps real.
    - SharePoint Online: aplicació inclosa a Microsoft 365 per a la gestió documental i com a repositori central de la base de coneixement corporativa. Permet l'organització, compartició i control d'accés als continguts de manera estructurada.
    - Azure AI Search: servei de cerca i indexació basat en IA que permet recuperar informació rellevant a partir de documents estructurats i no estructurats mitjançant tècniques de processament del llenguatge natural i anàlisi semàntica.
- IA i automatització
    - Microsoft Copilot Studio: entorn de desenvolupament per a la creació d'assistents conversacionals mitjançant una interfície gràfica, amb suport per a publicació en múltiples canals (web, missatgeria, etc.) i integració amb serveis externs.
    - Power Automate: plataforma per a la creació de fluxos de treball automatitzats entre aplicacions i serveis, amb capacitat per integrar sistemes interns i serveis de tercers mitjançant connectors predefinits o personalitzats.

- Azure OpenAI: servei que dona accés a models d'IA generativa, com GPT-4, a través d'API, amb capacitat per generar respostes i continguts a partir de diferents tipus d'entrada (text, imatges, fitxers, etc.) segons el model multimodal utilitzat.

- Anàlisi i visualització
  - Power BI: plataforma d'anàlisi de dades que permet crear informes i quadres de comandament interactius, útils per monitoritzar l'activitat dels assistents, identificar consultes recurrents i avaluar el rendiment i la qualitat de les respostes.

- CI/CD i gestió del cicle de vida del desenvolupament (DevOps)
  - Bitbucket: repositori corporatiu central de codi font basat en Git i element nuclear del model d'integració i desplegament continu (CI/CD) de l'Agència. Permet la gestió de versions, estratègies de ramificació estructurada, revisió de codi (pull requests), traçabilitat dels canvis i automatització de processos de build i integració.
  - Azure DevOps: plataforma utilitzada com a suport al procés de desplegament, especialment en entorns basats en Microsoft Azure. Pot actuar com a node intermedi per a l'orquestració de pipelines de desplegament, gestió d'entorns i automatització de lliuraments quan la naturalesa tècnica del projecte així ho requereixi.

1.2.3 Aplicacions existents

L'Agència disposa actualment de dos desenvolupaments tecnològics propis que donen suport a la governança i al compliment normatiu en matèria de ciberseguretat, i que constitueixen peces clau dins l'ecosistema digital de dades adreçat a oferir funcionalitats a les entitats del sistema de salut.

Eina d'Avaluació

- Resum funcional

Permet gestionar i executar processos d'avaluació del nivell de maduresa en ciberseguretat i del compliment normatiu de les entitats.

La plataforma processa qüestionaris configurables, integra les respostes capturades a través del Portal de Seguretat i incorpora la ingesta estructurada de resultats de proves tècniques de seguretat (*pentests*). Permet el seguiment evolutiu dels resultats i la generació d'indicadors i quadres de comandament per a la seva anàlisi i supervisió.

- Descripció tècnica
  - Aplicació web corporativa desplegada en entorn Microsoft Azure.
  - Arquitectura basada en microserveis.
  - Codi font allotjat al repositori corporatiu Bitbucket, integrat dins el model corporatiu de control de versions i CI/CD.
  - Desplegaments automatitzats mitjançant *pipelines* d'integració i desplegament continu sobre MS Fabric.
  - Integració amb el Portal de Seguretat per a la recepció estructurada de respostes de qüestionaris.
  - Mecanismes d'ingesta i processament de resultats de proves de penetració (*pentests*).
  - Exposició d'API per a integració amb sistemes corporatius.
  - Persistència de dades en bases NoSQL.

- Processos asíncrons per a càlculs i generació d'informes.
- Integració amb el Data Lake corporatiu per a explotació analítica i visualització d'indicadors.

Eina d'Adequació Normativa

- Resum funcional

Permet gestionar els processos d'adequació i certificació en ciberseguretat de les entitats mitjançant la recollida estructurada d'evidències de compliment normatiu.

La plataforma facilita la càrrega, organització i traçabilitat d'evidències associades als diferents requisits normatius, en realitza una validació assistida mitjançant intel·ligència artificial i dona suport a l'avaluació experta, generant informes i resultats del grau de compliment per entitat i esquema de certificació.

- Descripció tècnica
  - Aplicació web corporativa desplegada en entorn Microsoft Azure.
  - Arquitectura en capes (presentació, serveis i dades).
  - Codi font allotjat al repositori corporatiu Bitbucket, integrat dins el model corporatiu de CI/CD.
  - Desplegaments automatitzats mitjançant pipelines d'integració i desplegament continu sobre MS Fabric.
  - Motor d'avaluació assistida basat en serveis d'IA generativa per a la validació preliminar d'evidències.
  - Integració amb SharePoint com a repositori corporatiu d'evidències.
  - Integració amb el Data Lake corporatiu per a explotació analítica.
  - Model de dades estructurat en capes (*Bronze*, *Silver* i *Gold*).

Portal de Seguretat:

L'Agència disposa d'un Portal de Seguretat que actua com a punt únic d'interacció digital amb els diferents àmbits d'actuació de l'Agència (inclosos hospitals, centres sociosanitaris, salut mental i primària). Aquesta plataforma constitueix el canal corporatiu de relació amb les entitats i centralitza l'accés als serveis de ciberseguretat que presta l'Agència, actuant com a capa d'experiència d'usuari i d'accés unificat a l'ecosistema digital de serveis.

Qualsevol servei de dades, funcionalitat o nou desenvolupament adreçat a les entitats dels àmbits indicats haurà de preveure la seva canalització a través d'aquest portal com a mecanisme corporatiu d'interacció. No obstant això, el manteniment, evolució i desenvolupament del Portal de Seguretat resten fora de l'abast del present contracte.

- Descripció tècnica
  - Autenticació i autorització mitjançant integració amb sistemes corporatius d'identitat (VALId), amb control d'accés basat en rols i permisos.
  - Gestió diferenciada de perfils d'usuari amb segregació d'accés per entitat i responsabilitat.
  - Inici i gestió de processos vinculats als serveis de l'Agència.

- Formularis digitals per a la recollida estructurada de respostes i informació per part de les entitats.
- Càrrega, gestió i consulta d'evidències documentals.
- Consulta de l'estat dels expedients i recepció d'observacions i requeriments.
- Visualització de resultats d'avaluacions, anàlisis de vulnerabilitats i altres serveis actius.
- Integració de quadres de comandament i indicadors mitjançant Power BI.
- Incrustació d'aplicacions i mòduls funcionals dins la mateixa experiència d'usuari.
- Enviament automatitzat de notificacions mitjançant serveis de correu corporatiu (O365).

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 2.

Dins de dit lot s'inclouen les actuacions d'un servei de dades i analítica avançada en l'àmbit de la salut, 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 dades de ciberseguretat orientat a donar suport a l'Agència en l'exercici de les seves funcions en l'àmbit de la salut.

En concret, el present contracte basat té com a objecte la prestació d'un servei especialitzats per al disseny, desenvolupament, manteniment i evolució de solucions de dades de ciberseguretat amb la finalitat de donar suport a l'Agència en l'exercici de les seves funcions en relació amb la prestació de serveis en l'àmbit de la salut, especialment als hospitals, centres sociosanitaris, de salut mental i primària de Catalunya.

El contracte inclou, entre d'altres, la generació i manteniment de *pipelines* de dades, la integració de fonts d'informació internes i externes, el disseny i desenvolupament d'analítica avançada, indicadors i quadres de comandament, així com el desenvolupament, desplegament i manteniment de solucions basades en intel·ligència artificial generativa adreçades a les entitats usuàries.

Totes les prestacions objecte del contracte s'han de dur a terme en coordinació amb els serveis propis de l'Agència per garantir, en tot moment l'adequació als estàndards tècnics i normatius: alineament amb els criteris i models del servei de Govern de la dada; col·laboració amb el servei de Mitjans tècnics per al desplegament i operació de les solucions en la infraestructura corporativa; i compliment de les directrius establertes pel servei de Seguretat corporativa.

2.3 Objectius del servei

- Desenvolupar serveis de dades de ciberseguretat per al sector salut, orientats a hospitals, centres sociosanitaris, de salut mental i atenció primària, que transformin les dades en informació útil i accionable per a la gestió dels riscos de ciberseguretat.
- Posar a disposició de les entitats funcionalitats basades en dades, com ara quadres de comandament, indicadors operatius i serveis d'alertes, que facilitin una presa de decisions ràpida i informada davant amenaces de ciberseguretat.
- Processar i analitzar les dades de ciberseguretat mitjançant analítica avançada i intel·ligència artificial, amb l'objectiu de detectar patrons, riscos i amenaces rellevants i millorar la capacitat de resposta.
- Integrar tots els serveis i desenvolupaments en el portal de seguretat de l'Agència, com a entorn web únic d'accés i prestació del servei per a les entitats a les quals l'Agència ofereix suport.

- Facilitar l'ús efectiu dels serveis per part de les entitats usuàries, mitjançant un assistent amb intel·ligència artificial, documentació, formació i suport, promovent l'autonomia i l'apoderament en l'ús de la informació.

2.4 Característiques del servei.

El servei objecte del contracte es configura com un servei integral de dades de ciberseguretat per al sector salut, orientat al desenvolupament, operació i evolució de funcionalitats basades en dades que permetin generar informació operativa i accionable per als hospitals, centres sociosanitaris, de salut mental i atenció primària. Tots els serveis i desenvolupaments s'integraran en el portal de seguretat de l'Agència, com a entorn web únic d'accés i prestació del servei.

Les característiques essencials del servei són les següents:

2.4.1 Organització del servei

El servei haurà de disposar d'una organització sòlida i adaptable que permeti garantir la correcta execució de les prestacions al llarg de tota la vigència del contracte. L'adjudicatari haurà de definir un equip de treball adequat en nombre i composició, amb una assignació clara de responsabilitats, que asseguri la cobertura de les necessitats del servei i la seva capacitat d'evolucionar davant canvis en la demanda.

Aquesta organització haurà d'estar suportada per un model de funcionament que permeti estructurar les activitats, coordinar els diferents rols implicats i assegurar una relació fluida amb les unitats corporatives de l'Agència, facilitant la integració del servei dins l'ecosistema existent.

El servei haurà d'incorporar dinàmiques de treball que afavoreixin la col·laboració entre equips, la compartició de coneixement i l'alineament amb els objectius definits, amb l'objectiu de garantir una execució eficient i orientada a resultats als usuaris de l'Agència i de les entitats de salut.

Així mateix, caldrà preveure mecanismes que permetin gestionar situacions no planificades, ajustar la prestació del servei quan sigui necessari i garantir la seva continuïtat en escenaris adversos, mantenint en tot moment els nivells de qualitat requerits.

2.4.2 Metodologia de treball

La prestació del servei s'haurà de dur a terme mitjançant una metodologia de treball estructurada i adaptada a l'explotació continuada de dades en entorns de ciberseguretat, que permeti planificar, executar i fer el seguiment de les actuacions amb criteris de qualitat, control i traçabilitat.

La metodologia haurà d'integrar els processos de desenvolupament i evolució de les solucions, incloent la definició de mecanismes de validació i proves que assegurin la qualitat dels resultats i la seva adequació als requisits del servei.

Al llarg de tot el cicle de vida, s'haurà de garantir el compliment dels requisits normatius aplicables i de les directrius corporatives de l'Agència, així com la qualitat i fiabilitat de les dades i dels processos de tractament.

El servei haurà d'incorporar també mecanismes d'operació que permetin el seguiment de l'activitat, la gestió d'incidències i la continuïtat del servei, així com assegurar que els productes de dades siguin utilitzables pels diferents perfils d'usuari.

Finalment, s'hauran d'establir processos de documentació i transferència del coneixement que permetin mantenir la traçabilitat i assegurar la continuïtat i evolució del servei.

2.4.3 Solució tècnica

La solució tècnica haurà de concebre's com un conjunt integrat i coherent de components, alineat amb l'ecosistema tecnològic de l'Agència, que garanteixi la seva compatibilitat i interoperabilitat amb les plataformes, serveis i tecnologies existents. Aquesta integració haurà de permetre una incorporació natural de les noves funcionalitats dins l'entorn corporatiu, evitant dependències innecessàries i assegurant la seva sostenibilitat.

L'arquitectura s'haurà de basar en principis de modularitat i desacoblament, facilitant tant la seva evolució progressiva com l'adaptació a nous requeriments funcionals, increments de volum de dades o creixement en el nombre d'usuaris, tot mantenint els nivells de servei, disponibilitat i rendiment exigits.

En aquest marc, la solució haurà d'incorporar una plataforma de dades que permeti gestionar de manera eficient el cicle complet de les dades, des de la ingesta fins a la seva explotació, assegurant la seva operació mitjançant capacitats de monitorització, control i desplegament continu dels pipelines i desenvolupaments, d'acord amb els estàndards corporatius.

Així mateix, es preveu la incorporació de capacitats avançades orientades a l'optimització de processos i a la generació de valor a partir de les dades, mitjançant l'ús de tecnologies com la intel·ligència artificial, l'aprenentatge automàtic o altres mecanismes d'automatització. Addicionalment, ha de facilitar la integració de noves fonts d'informació, tant internes com externes, per tal d'enriquir les dades disponibles i millorar el context i la utilitat dels resultats generats.

2.5 Activitats del servei

- **Generació i manteniment de *pipelines* de dades.** Disseny, desenvolupament, operació i manteniment de pipelines per a la ingestió, processament, transformació i explotació de dades de ciberseguretat, garantint la seva qualitat, traçabilitat i disponibilitat, així com la seva alineació amb el model de govern de la dada de l'Agència, incloent la gestió de metadades, classificació i control dels actius de dades.

- **Manteniment dels sistemes de dades associats a les aplicacions existents**. Operació i manteniment dels entorns i components tecnològics que suporten les aplicacions existents de suport a la governança i compliment normatiu per a les entitats de salut: l'Eina d'Avaluació i l'Eina d'Adequació Normativa (1.2.3. Aplicacions existents). El servei haurà de garantir la continuïtat, la compatibilitat amb els sistemes i l'alineació amb els estàndards d'arquitectura, seguretat i governança de la dada.

- **Desenvolupament de noves aplicacions de dades.** Disseny, desenvolupament i desplegament de noves aplicacions o funcionalitats per a la captura, tractament i explotació de dades, integrades amb l'ecosistema tecnològic de l'Agència. Les solucions hauran d'incorporar pràctiques de desplegament continu (CI/CD) i complir amb els estàndards d'arquitectura, seguretat i govern de la dada.

- **Analítica avançada per al disseny de nous indicadors i quadres de comandament.** Aplicació de tècniques d'analítica avançada sobre les dades de ciberseguretat disponibles per al disseny, definició i evolució d'indicadors operatius i quadres de comandament orientats a la presa de decisions.

- **Integració de noves fonts de dades i ingestió d'informació.** Integració progressiva de noves fonts internes i externes de dades, incloent-hi les respostes estructurades als qüestionaris del Portal de Seguretat adreçats a les entitats usuàries. El servei haurà de garantir la seva correcta ingesta, normalització i integració amb els *pipelines* de dades existents per al seu processament, explotació analítica i generació d'informació operativa.

- **Compliment normatiu i seguretat aplicada a dades.** Aplicació de mesures de seguretat i compliment normatiu en l'àmbit de les dades. Implementació i seguiment de controls de seguretat, classificació de la informació, control d'accessos i altres mesures necessàries per garantir el compliment de l'ENS, RGPD i les directrius corporatives.

- **Desenvolupament i manteniment d'un assistent basat en IA generativa.** Desenvolupament, desplegament i manteniment d'un assistent amb IA generativa integrat al portal de seguretat, orientat a facilitar la consulta d'informació, indicadors i documentació, així com el suport a l'ús de les funcionalitats del servei.

- **Formació a les entitats per donar suport a l'ús del portal.** Realització d'accions formatives i de suport adreçades a les entitats usuàries per facilitar l'adopció i l'ús efectiu del portal de seguretat i de les funcionalitats basades en dades.

- **Coordinació amb els serveis de l'Agència**. Coordinació contínua amb els serveis corporatius de l'Agència, en particular amb els equips de govern de la dada, Portal de seguretat i enginyeria de dades, per garantir l'alineació tècnica, la coherència del servei i el compliment dels estàndards corporatius.

2.6 Lliurables del servei

- **Models de dades.** Models de dades de ciberseguretat definits i estructurats, integrats en els *pipelines* de dades de l'Agència, que permetin el processament, explotació i evolució de la informació. Aquests models hauran d'estar documentats, versionats i alineats amb els criteris corporatius de qualitat, traçabilitat i govern de la dada.

- **Actius de govern de la dada integrats a l'eina corporativa.** Diccionaris de dades, glossaris, metadades, classificacions i relacions entre actius de dades integrats en l'eina corporativa de govern de la dada de l'Agència, assegurant la traçabilitat, comprensió i reutilització de la informació generada.

- **Quadres de comandament de ciberseguretat.** Quadres de comandament operatius integrats en el portal de seguretat de l'Agència, que permetin la visualització d'indicadors i informació de ciberseguretat rellevant per a les entitats del sector salut. Els quadres hauran de ser funcionals, accessibles segons perfil d'usuari i orientats a la presa de decisions.

- **Mòdul d'indicadors de monitorització i alertes.** Un mòdul d'alertes integrat en el portal de seguretat, amb alertes configurades i operatives en temps gairebé real, basades en dades, indicadors i llindars definits, orientades a la detecció, notificació i seguiment de situacions de risc o amenaça de ciberseguretat.

- **Interfícies de programació d'aplicacions (API).** Disseny i implementació d'API operatives per al consum de dades i serveis per part de sistemes interns de l'Agència o, si escau, de sistemes externs autoritzats, complint en tot moment amb les mesures de seguretat, control d'accés i traçabilitat establertes per l'Agència.

- **Arquitectura i interfície d'un assistent amb intel·ligència artificial generativa.** Desenvolupament del sistema i la interfície integrada al Portal de seguretat per a un assistent basat en intel·ligència artificial generativa, orientat a la consulta d'informació, indicadors i documentació, així com al suport a l'ús dels serveis de dades de ciberseguretat.

- **Documentació del servei.** Documentació tècnica i funcional completa i actualitzada dels serveis prestats, incloent, com a mínim, la documentació de l'arquitectura de dades, els models de dades, els indicadors, les funcionalitats desenvolupades, les API i les guies d'ús i explotació del servei.

- **Actius de govern de la dada integrats a l'eina corporativa.** Diccionaris de dades, glossaris, metadades, classificacions i relacions entre actius de dades integrats en l'eina corporativa de govern de la dada de l'Agència, assegurant la traçabilitat, comprensió i reutilització de la informació generada.

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.
- 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.

Es 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.

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
Project Manager	Encarregat de planificar, fer seguiment, prestar suport, acompanyament i assessorament en la gestió, de programes i projectes de consultoria en l'anàlisi i tractament de les dades, per a la creació, manteniment, evolució i millora de solucions transversals de ciberseguretat, i la millora de l'eficiència de les activitats i processos. Responsable del desenvolupament de plans d'evolució i millora de la maduresa de les solucions d'analítica de dades i de metodologies de gestió d'iniciatives i projectes en l'àmbit de les dades, aportant coneixement expert en aspectes tecnològics, procedimentals, de qualitat, seguretat, costos i beneficis.
Científic de dades	Desenvolupament de models de decisió, multidimensionals i models associatius. Neteja i exploració de les dades, creació de models algorítmics i creació de nou coneixement en base a les dades. Construcció de models per l'analítica de dades i desenvolupament de models predictius.
Consultor de visualitzacions de dades	Desenvolupament i desplegament de solucions/projectes vinculats a la visualització i anàlisi de dades (BI, ETL, Quadres de Comandament, Visualitzacions, integracions,...)
Enginyer de dades	Desenvolupament i manteniment dels models de dades, evolucionant-los segons les necessitats de l'Agència. Desenvolupament, construcció, test i manteniment de l'arquitectura i els pipelines. Assegurament de la qualitat i seguretat de les dades, implementant mesures per garantir la integritat, confidencialitat i disponibilitat de les dades.
Tècnic/ Desenvolupador	Programació de processos de càrrega, integracions i automatitzacions vinculades a les dades, aplicacions existents i la seva automatització. Desenvolupaments necessaris per d'automatitzar el repte del servei, aplicar mesures de seguretat i mecanismes d'integració entre sistemes. Desenvolupament i desplegament de solucions d'Intel·ligència artificial.

De conformitat amb la Memòria i el PCAP, s'haurà 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 **5.074,43 hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	% dedicació	Hores
Project Manager	5%	253,72
Científic de dades	25%	1.268,61
Consultor de visualitzacions de dades	25%	1.268,61
Enginyer de dades	30%	1.522,33
Tècnic/ Desenvolupador	15%	761,16
	100%	**5.074,43**

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

3.3.1 Perfils

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

Perfil	Requisits
Project Manager	5 anys d'experiència mínims
Científic de dades	3 anys d'experiència mínims
Consultor de visualitzacions de dades	
Enginyer de dades	
Tècnic/ Desenvolupador	

S'entén que aquests perfils es corresponen amb els rols que, des de l'Agència, s'identifiquen per la prestació d'aquest servei.

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. L'adjudicatari 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 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 continua, 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 adjudicataris 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 de l'adjudicatari, 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 capacitació 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 capacitació 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.

3.14.6 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 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.

