Plec de prescripcions tècniques particulars que regeix la contractació basada relativa al suport a la Governança de l'operació de l'Àrea d'Operacions

Exp. CB24AMCONSL1B003

Índex

1 Introducció 4

1.1 Funcions de l'Agència de Ciberseguretat de Catalunya rellevants a efectes del la nova estratègia de contractació 4

2 Descripció dels serveis objecte de la contractació basada. 6

2.1 Context dels serveis objecte de la licitació. 6

2.2 Serveis del contracte basat. 6

2.2.1 Objecte i abast dels serveis. 6

2.2.1.1 Gestió del Coneixement intern. 7

2.2.1.1.1 Definició i manteniment del model de dades operatiu i de context 8

2.3 Gestió de la informació del context operatiu 9

2.3.1.1.1 Gestió de la informació operativa de ciberseguretat 9

2.3.1.2 Govern de l'operativa 10

2.3.1.2.1 Disseny i manteniment de models de relació interns 10

2.3.1.2.2 Gestió i seguiment de la demanda 11

2.3.1.2.3 Orquestració operativa 11

2.3.1.2.4 Suport en el seguiment d'objectius estratègics i tàctics 13

2.3.1.2.5 Coordinació davant esdeveniments puntuals de seguretat 13

2.3.1.3 Entrega de valor 15

2.3.1.4 Volumetries actuals 16

2.3.1.5 Lliurables del servei 17

2.3.1.6 Mètriques i indicadors 18

2.3.2 Característiques del servei. 19

3 Condicions d'execució del servei 20

3.1 Horaris 20

3.2 Localització física. 20

3.3 Equip de treball 20

3.3.1 Perfils 22

3.4 Canvi de recurs 23

3.5 Control de rotació 24

3.6 Eines i equipament per a la prestació de serveis. 24

3.7 Gestió del coneixement 25

3.8 Seguretat Corporativa 25

3.9 Control de Gestió 26

3.10 Documentació. 27

3.11 Formació 27

3.12 Contingència 27

3.13 Metodologia, estàndards i lliurables 28
3.14 Seguretat 28
3.14.1 Deure de confidencialitat 28
3.14.2 Dades de caràcter personal 28
3.14.3 Compliment del marc legal de ciberseguretat i del marc normatiu intern 28
3.14.4 Capacitat tècnica 29
3.14.5 Adquisició de productes/eines i productes o serveis de seguretat 29
3.14.6 Interconnexions 29
3.14.7 Verificació del compliment i auditoria 30
3.14.8 Incidents de seguretat 30
3.14.9 Accés a la informació 30
3.15 Assegurament i control de la qualitat i la millora contínua 30
3.16 Seguiment del servei 31
3.17 Integració amb altres equips 32
3.18 Compromís amb el talent femení 32

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

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

.

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 de 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 Ciberseguretat 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.

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 per l'entrega de serveis de consultoria per a l'Agència de Ciberseguretat de la Generalitat de Catalunya, estructurat en 2 lots: Lot 1: Serveis de Consultoria de Ciberseguretat inclosa la vessant d'arquitectura, i Lot 2: Serveis de consultoria d'analítica de dades.

Concretament s'emmarca en el: Lot 1 - Consultoria de Ciberseguretat inclosa la vessant d'arquitectura.

Dins d'aquest lot s'inclouen els següents àmbits de treball: Gestió del coneixement intern, govern de l'operativa de ciberseguretat i entrega de valor de l'Àrea d'Operacions, els quals son objecte de la present licitació.

De totes les àrees que formen l'Agència de Ciberseguretat de Catalunya, l'Àrea d'Operacions (en endavant AOS), s'encarrega d'executar mesures operatives específiques per prevenir la materialització de les ciberamenaces dins dels àmbits d'actuació i de respondre, quan sigui necessari, per a reduir al màxim la seva afectació si l'incident arriba a materialitzar-se.

El servei de Governança de l'operació de l'AOS de l'Agència, té la finalitat de millorar la gestió administrativa, els processos de monitorització i la valoració dels serveis que genera l'activitat de dita àrea. El servei inclou àmbits com la Gestió del Coneixement, el Govern de l'Operativa i l'Entrega de Valor, regits per principis com la coordinació entre equips operatius, la garantia d'informació de qualitat, la gestió àgil de la demanda, la generació de resultats alineats amb els objectius de l'Agència, i la capacitat d'autonomia i lideratge de l'Àrea.

Els objectius del servei inclouen establir la Governança de l'operativa com un referent per canalitzar sol·licituds de seguretat, proveir coneixement rellevant derivat de l'activitat operativa, facilitar informació contextual sobre ciberamenaces, i definir un model de gestió de la demanda. També té com a funció liderar l'orquestració dels serveis per optimitzar la resolució dels focus operatius, implementar quadres de comandament estratègics i tàctics per a una presa de decisions àgil, i garantir que la ciberamenaça sigui un element central en l'activitat de l'AOS.

2.2 Serveis del contracte basat.

2.2.1 Objecte i abast dels serveis.

L'objecte del següent basat es focalitza en la prestació d'un servei de suport a la Governança de l'operació de l'AOS de l'Agència.

La finalitat de l'equip de Governança de l'operació de l'AOS és prestar un servei transversal de qualitat per la gestió de les tasques administratives necessàries, així com els processos de monitorització i presentació del valor, que els diferents serveis generen amb la seva activitat.

El servei de governança de l'AOS està composat pels següents àmbits de treball:

▪ **Gestió del Coneixement intern** per tal de disposar de la informació de context necessària per poder respondre de manera eficient a qualsevol ciberamenaça que afecti als actius dins de l'àmbit de responsabilitat de l'AOS.

▪ **Govern de la operativa de l'AOS** per tal de assegurar la correcta comunicació entre els diferents equips de l'Àrea, establint els procediments necessaris de coordinació operativa entre els diferents serveis de l'AOS, garantint la compartició d'informació entre aquests, i actuant com a principal punt de contacte de l'Àrea amb els àmbits de l'Agència.

▪ **Entrega de Valor** de l'AOS respecte del reptes aconseguits i els beneficis que representen cap a la direcció de l'Agencia.

Així mateix, el servei de suport a la Governança d'operació de la seguretat també té fins a 5 principis transversals que regeixen el seu disseny:

- El servei **focalitzarà** la seva capacitat en **governar la coordinació** entre els diferents equips operatius de l'AOS, vetllant per l'assoliment conjunt dels objectius estratègics i tàctics de l'Agència.
- En aquesta línia, el servei ha de **garantir que els serveis** de l'AOS **disposen d'informació de context de qualitat** per facilitar la gestió i resposta adient a les ciberamenaces.
- De la mateixa manera, el servei ha de desenvolupar els processos oportuns per oferir una **gestió àgil de la demanda** dirigida a l'AOS.
- El servei **potenciarà missatges de valor** respecte els resultats de l'activitat operativa de tot l'AOS, alineats amb la seva aportació al negoci i l'eficiència de l'operació de la seguretat.
- El servei ha de ser **autònom** amb capacitat de lideratge i de **defensa dels interessos de l'Agència**.

Finalment, es destaquen els objectius globals del Servei que s'han d'assolir en la seva prestació, tenint en compte l'orientació cap a resultats que s'espera:

- Situar la funció de "Governança de l'operativa" com a referent dins de l'AOS i l'Agència per canalitzar qualsevol sol·licitud o petició referent a l'operació de la seguretat.
- Establir els **canals oportuns amb cadascun dels àmbits** per proveir coneixement generat arrel del 100% de l'activitat operativa rellevant.
- Establir els **canals oportuns** amb **cadascuna de les àrees de l'Agència** per disposar i proveir **informació de context** rellevant de les ciberamenaces aplicables en base al coneixement del negoci i l'activitat operativa.
- Definir i documentar els **models de gestió de la demanda** pels **principals tipus de peticions rebudes a l'AOS** (serveis inclosos al catàleg de serveis, peticions de CTTI, peticions de tercers, actualitzacions de programari, sol·licituds d'incidències i peticions de noves eines o recursos).
- Liderar l'**orquestració dels serveis** per minimitzar el temps màxim per la resolució dels focus operatius gestionats per l'AOS.
- Dotar de la **capacitat de decisió de manera àgil** a l'AOS basada en el disseny, suport en la implantació, i millora de quadres de comandament estratègics i tàctics.
- Actualitzar i mantenir **els processos de gestió de la dada** per a la informació operativa més rellevant per l'AOS.
- Garantir la **ciberamenaça com a element vehicular** de l'activitat operativa de l'AOS.

A continuació es detallen els elements, característiques i objectius dels tres àmbits de treball del servei de governança de l'AOS, i que la companyia adjudicatària del present Basat haurà de tenir en compte a l'hora de prestar el seu servei de suport.

2.2.1.1 Gestió del Coneixement intern.

La funció de gestió i coneixement intern del servei de Governança de l'operació de la seguretat de l'AOS tindrà com a principals funcions la definició i el manteniment del model de dades operatiu i de context, la qual assegurarà una estructura sòlida i coherent per a la gestió de la ciberseguretat; la gestió de la informació del context operatiu, la qual integrarà les dades rellevants sobre l'entorn i les amenaces per millorar la presa de decisions de l'AOS; i la gestió de la informació operativa de ciberseguretat, la qual consolidarà i estructurarà les dades generades per les operacions de seguretat per garantir-ne la disponibilitat, traçabilitat i utilitat d'aquestes.

2.2.1.1.1 Definició i manteniment del model de dades operatiu i de context

Cal definir i mantenir un model de govern que permeti aconseguir el màxim valor de les dades tractades per l'AOS, donant suport a tots els nivells possibles, des de la presa de decisions a la recerca de noves solucions i models d'operació de la seguretat alineats amb els objectius estratègics de l'Agència.

La definició del model s'ha de dur a terme per permetre respondre a aspectes rellevants sobre la pròpia gestió de la dada i el seu cicle de vida, què com a mínim inclourà les següents tasques:

- Identificació de la informació mínima requerida per garantir una correcta operació de la seguretat dels actius dins de l'abast, procurant estandarditzar la tipologia de dades per tots els actius de les mateixes característiques.
- Classificació i priorització de les dades requerides per l'AOS per acomplir les seves funcions operatives.
- Coordinació amb els equips tècnics corresponents per assegurar que les bases de dades i repositoris de l'AOS inclouen tota la informació requerida.
- Identificació de les fonts origen considerades vàlides per la recollida de les dades d'interès i definició dels canals/fluxos/mètodes establerts per actualitzar-la, on les fonts poden ser sistemes d'informació o equips de treball d'alguna de les àrees de l'Agència o de tercers.
- Identificació de responsables o propietaris de la informació de les fonts de dades definides.
- Definició de criteris per al manteniment i conservació de la informació, incloent el període d'actualització, vigència i/o retenció. Aquest criteris hauran de complir els requeriments normatius o legals que puguin limitar o determinar els mètodes de tractament d'acord amb les directrius que marqui l'àrea corresponent de l'Agència.
- Identificació de les persones, serveis de l'Agència o ens als quals donar accés a la informació, ja sigui de manera directa amb accés als repositoris de l'AOS (permisos de lectura o edició, depenent del cas), o compartint amb aquests contingut més estàtic i estructurat (p.ex. Fets rellevants, butlletins i informes mensuals).

Actualment, l'Agència gestiona un entorn molt complex on conviuen una gran varietat d'entorns tecnològics i usuaris dels sistemes d'informació, entre els quals destaquen els departaments de la Generalitat de Catalunya, els seus organismes autònoms, Centre de Telecomunicacions i Tecnologies de la Informació (CTTI), entitats del sector públic de la Generalitat A la vegada, l'Agència necessita interactuar contínuament amb diferents interlocutors, tant de negoci (departaments i els seus responsables de seguretat - RSIs), com altres àrees de l'Agència, com els diferents ens que composen el sector públic de Catalunya.

D'igual forma, l'Agència, disposa d'un inventari de solucions de ciberseguretat, que agrupa les diferents solucions de ciberseguretat desplegades tant pels departaments de la Generalitat de Catalunya, com per la pròpia entitat en l'entorn corporatiu de l'Agència, el qual requereix un manteniment i actualització constant.

Per tot plegat, el servei licitat haurà de donar suport en la implementació dels mecanismes necessaris per assegurar que la resta d'equips de l'AOS de l'Agència de Ciberseguretat disposin, en tot moment, d'informació complerta i rellevant sobre l'actualitat arreu dels àmbits d'actuació que pugui condicionar les tasques operatives i el seu esdevenir.

Per acomplir l'objecte d'aquest servei de Gestió del Coneixement, es contemplen les següents activitats:

- Gestió de la informació del context operatiu.
- Gestió de la informació operativa de la Ciberseguretat.

A continuació s'exposen aquestes dues activitats.

2.3 Gestió de la informació del context operatiu

- **Identificació i registre de la dada de context**

Amb l'objectiu de poder identificar i poder respondre de manera eficient a qualsevol ciberamenaça que afecti als actius inclosos en l'àmbit de responsabilitat de l'Agència, és primordial que l'AOS disposi del coneixement adient per entendre el context dels mateixos. En aquest sentit, és responsabilitat del servei assegurar que es disposa de la informació necessària i actualitzada, la majoria provinent d'altres àrees de l'Agència, i garantir que aquesta està disponible per la resta de funcions de l'AOS.

Així, i entre d'altres, caldrà dur a terme la gestió continuada de la informació mínima i de la seva classificació per cada actiu, ja siguin inventaris de persones (Alts càrrecs, altres empleats dels ens públics) o de sistemes d'informació (crítics i no crítics) dels àmbits d'actuació responsabilitat de l'Agència. Addicionalment, arrel de la relació amb negoci, s'haurà de poder identificar possibles esdeveniments crítics susceptibles de requerir accions especials durant l'operativa dels serveis operatius (per exemple períodes d'eleccions, preinscripcions universitàries o adjudicació de places públiques, i esdeveniments especials com el Mobile World Congress o la Copa Amèrica), identificar canvis de responsables de seguretat departamentals, entre d'altres.

- **Coordinació amb tercers per l'obtenció d'informació de context**

Caldrà generar i automatitzar de la manera més eficient possible la recollida i manteniment de la informació externa prèviament identificada (inventaris i altra informació de context) per assegurar què estiguin actualitzats i siguin consumibles pels serveis operatius de l'AOS. Per fer-ho, serà important disposar d'un model de relació establert, tenir capacitat de coordinació amb tercers responsables de les dades de context, i coordinar els diferents equips involucrats que permetin la ingesta o modificació de dades directament des de les diferents fonts internes dels serveis de l'Agència que contenen aquesta informació.

- **Control de qualitat i manteniment de la informació del context**

Caldrà definir i implementar els processos i controls adients per garantir la qualitat de la informació de context als repositoris de l'AOS, aixi com amb la funció de govern de la dada de l'Agencia de Ciberseguretat de Catalunya responsable de centralitzar i explotar les dades rellevants de l'entitat . En cas de trobar o sospitar que un actiu no està correctament actualitzat i/o no es té visibilitat sobre alguns camps, cal definir clarament el mètode/canal de notificació amb els responsables de la dada i se'ls ha d'avisar per tal que comprovin l'estat de l'actiu i l'actualitzin si és necessari.

2.3.1.1.1 Gestió de la informació operativa de ciberseguretat

- **Identificació i registre de la dada operativa**

Com a part de l'activitat operativa de les funcions de l'AOS aquestes generen gran quantitat d'informació de valor. És responsabilitat d'aquesta funció assegurar que els equips operatius responsables registren adequadament tots els esdeveniments de seguretat produïts i gestionats per la seva part, així com analitzar-los des de un punt de vista més tàctic per identificar possibles tractaments agregats, necessitats de creuament de dades, i en general facilitar el coneixement de la situació de seguretat dels actius en tot moment.

Caldrà dur a terme el seguiment i millora continua del registre de l'activitat operativa de les funcions de l'AOS, essent necessari generar la informació diària de l'estat de seguretat dels actius i facilitar que sigui accessible de manera àgil per a les parts que es defineixin.

A tall d'exemple, s'haurà de disposar d'informació mínima de tots els atacs, incidents, amenaces i vulnerabilitats gestionades pels diferents equips que conformen les funcions de l'AOS, permetent identificar el més crític, tipologia, origen, o els actius afectats.

- Caldrà generar i automatitzar els inventaris i la seva informació associada provinent de les diferents eines que continguin informació dels mateixos i la seva activitat operativa relacionada (eina de tiqueting, bases de dades internes, Consoles d'Antivirus, Filtrat de continguts, SIEM, entre d'altres) per tal de que estiguin actualitzats i siguin accessibles per a la resta dels serveis operatius o altres consumidors que es defineixin. Per fer-ho, el servei s'haurà de coordinar amb l'equip intern de l'AOS de l'Evolució de Solucions per garantir la definició d'un model de dades adient i la integració tecnològica adient per mantenir tots els registres necessaris en els repositoris de l'AOS. **Control de qualitat i manteniment de la informació operativa**

Al igual que es farà amb la informació provinent de tercers fora de l'AOS, també caldrà definir i implementar els processos i controls adients per garantir la qualitat de la informació generada per la pròpia operativa de les funcions de l'AOS i el seu registre als repositoris de l'AOS.

En cas de trobar o sospitar que alguna informació no està correctament actualitzada i/o no es té la visibilitat adient que permeti generar valor i transmetre els resultats de les funcions de l'AOS, cal definir clarament el mètode/canal de notificació i coordinació amb les funcions responsables i avisar-los per tal que comprovin l'estat de la mateixa i l'actualitzin, en cas de ser necessari.

2.3.1.2 Govern de l'operativa

La funció de govern de l'operativa del servei de Governança de l'operació de la seguretat de l'AOS tindrà com a principals funcions el disseny i manteniment dels models de relació interns, els quals hauran de garantir una col·laboració eficient entre les diferents àrees de l'AOS; la gestió i el seguiment de la demanda operativa, els quals hauran d'assegurar una resposta alineada amb les necessitats de l'AOS; l'orquestració operativa, la qual facilitarà la coordinació entre equips i processos, alhora que donarà suport en el seguiment dels objectius estratègics i tàctics de l'AOS; i la coordinació davant esdeveniments puntuals de ciberseguretat, garantint una resposta efectiva i estructurada.

2.3.1.2.1 Disseny i manteniment de models de relació interns

Serà funció d'aquest servei la definició dels mecanismes adients que permetin assegurar la correcta comunicació entre els diferents equips operatius de l'AOS, així com garantir la compartició d'informació de manera bidireccional amb les parts que s'acordin.

Com a mínim, haurà d'encarregar-se de les següents activitats:

- Identificació de serveis interns o externs de l'AOS amb els que interaccionar de manera periòdica per compartir informació operativa o de context.
- Identificació d'aspectes a tractar i informació a compartir amb cadascun dels serveis interns o externs de l'AOS amb els que s'identifiqui interacció periòdica.
- Determinació dels fluxos i canals de comunicació a utilitzar entre les parts interessades, incloent la formalització d'un model de relació que s'haurà de mantenir actualitzat durant la prestació del servei.

2.3.1.2.2 Gestió i seguiment de la demanda.

Serà funció administrativa d'aquest basat, la gestió i operació d'un servei de suport a la gestió de la demanda de l'AOS, per tal de donar el suport administratiu a la resta de serveis de l'AOS portant a terme activitats com les següents, entre d'altres:

- **Actuar com a punt principal de contacte de l'AOS de l'Agència** (correu electrònic, eines de gestió de tiqueting, atenció telefònica), i **canalitzar els casos rebuts cap als equips corresponents dins o fora del mateix**.
- Assegurar la capacitat de **mantenir informats als actors afectats pels serveis de l'Agència del progrés i estat de situació** de les seves peticions.
- **Canalitzar les principals comunicacions de l'AOS r**elacionades amb l'operació de la seguretat i la prestació dels serveis de catàleg (notificació d'intervencions, alertes especials, i gestió dels serveis de subscripcions).
- **Canalitzar les comunicacions entre l'Agència i el seus '*partners*' tecnològics** (CTTI, AOC, IMI, entre d'altres) per a la seva integració operativa, a partir de les eines acordades entre les parts.
- **Fer la gestió dels formularis i el control de la qualitat** de les dades d'entrada als processos de provisió de serveis (peticions, incidències i RFCs.)
- **Actuar com a taula de canvis i incidències** per tal de fer el seguiment per a la resolució de les mateixes.
- **Analitzar de manera recurrent el conjunt de la demanda tractada pels serveis de l' AOS** per:
    - Fer seguiment de l'estat de les peticions d'execució de serveis de l'AOS per garantir de manera general la prestació de serveis de qualitat.
    - Garantir el correcte compliment dels fluxos definits per la gestió de la demana.
    - Donar suport a la presa de decisions en relació a la seva classificació, priorització.
    - Identificar possibles ineficiències o punts de millora en la gestió de la demanda.
- **Col·laborar en l'estandardització i automatització** de les tasques més repetitives del servei de Suport a la Gestió de la Demanda de l'AOS com objectiu del guany d'eficiència dels recursos del servei, p.e. la gestió dels tiquets de les eines de gestió de la demanda de l'AOS.

Amb aquestes directrius, l'equip adjudicatari haurà de considerar el desenvolupament de funcions d'administració del servei, tant de l'organització interna, així com de les relacions amb la resta d'equips de l'Agència. Aquestes funcions s'hauran de focalitzar en el suport i l'assessorament a nous projectes i canvis, ajudant amb el seu coneixement, proves i investigació a la transformació de la mateixa Agència.

2.3.1.2.3 Orquestració operativa

La orquestració operativa és un dels procediments operatius claus de l'AOS i té com a objectiu principal **establir els procediments necessaris per garantir la coordinació operativa entre els diferents serveis de l'AOS i assegurar la consecució dels objectius generals de la mateixa**, **i el focus a les tasques de major rellevància global.** En tot cas, ha de garantir la prevenció,

protecció, detecció i resposta davant les diferents ciberamenaces que puguin afectar a la Generalitat de Catalunya.

Actualment, la orquestració operativa de l'AOS és un procés ja establert, el qual es desenvolupa mitjançant l'execució de reunions diàries les quals són coordinades pel present servei (actualment a les 11:00h i 16:30h). En aquestes reunions hi participen totes les funcions de l'AOS, i es determina a la primera de les mateixes els principals focus de treball de l'àrea durant el dia, en funció de les principals ciberamenaces aplicables. A la segona reunió s'analitza tant l'evolució de les tasques que s'han definit dintre dels focus operatius, així com el seu tancament.

Finalment, el resum de les principals tasques executades durant el període són recollits en un document denominat "Fets Rellevants", el qual és distribuït internament a l'Agència.

D'igual forma, l'Orquestració Operativa determina les activitat de focus diari distingint entre 3 àmbits principals:

▪ **Focus operatiu**. Totes aquelles tasques implicades en l'operativa diària dels serveis de l'AOS, dirigides a complir els objectius de l'Agència (gestió i protecció davant atacs, gestió i resposta a incidents, gestió d'amenaces o comitès de crisi).

▪ **Focus Evolutiu**. Totes tasques dirigides a millorar l'eficiència de l'operativa dels serveis i en general millorar la maduresa de l'AOS.

▪ **Focus Incidental**. Totes aquelles tasques dirigides a resoldre incidències identificades sobre les eines què utilitzen els serveis en la seva operativa diària.

Per tot plegat, els principals àmbits a assolir en la funció d'orquestració són:

- **Rol de coordinació entre els serveis operatius.**

El servei licitat s'ha d'encarregar de governar, dirigir i moderar aquestes reunions d'orquestració, vetllant per a que les activitats acordades dirigides a resoldre els diferents focus definits es duen a terme correctament, sense contratemps, i mantenint sempre un alineament i un objectiu comú entre els equips d'operacions.

D'igual forma, serà funció del rol de coordinació el suport a la resolució de conflictes operatius que es puguin donar entre els serveis, vetllant en tot cas pels interessos globals de l'AOS.

Addicionalment, s'ha d'encarregar de definir els processos que regiran les relacions entre els equips d'operacions, on es tractaran, per exemple, el canal i la metodologia per realitzar una sol·licitud d'execució d'una operació o la modificació d'una operativa. A la vegada, haurà de vetllar pel correcte desplegament dels procediments establerts, definint els indicadors necessaris per monitoritzar el grau de desplegament.

Com a suport indispensable a aquest rol, es troba la funció d'Intel·ligència Operativa, amb la qual el servei s'haurà de coordinar en tot moment per assegurar que les tasques realitzades per l'AOS són òptimes per prevenir l'amenaça i respondre diligentment als incidents.

- **Generació de procediments i fitxes d'orquestració**.

L'adjudicatari haurà de garantir que cada àrea aporta la informació necessària i de qualitat per omplir les fitxes requerides per a cada focus tractat en la orquestració. Aquestes fitxes són un resum de l'activitat generada i fites planificades-assolides per cada servei en relació a les tasques establertes a cada orquestració. L'adjudicatari podrà proposar nous formats per la realització de la present tasca.

Igualment, serà funció del present servei la definició i formalització dels procediments d'orquestració implementats durant la prestació del servei.

- **Visió general dels serveis d'operacions i proposta de millores.**

La funció d'Orquestració Operativa ha de treballar per tenir una visió general de l'operativa dels serveis d'operacions i ha de proposar millores, tant per al seu propi servei com per als altres, per tal d'arribar a la màxima cohesió, eficàcia i precisió en l'operativa global de l'AOS.

- **Alineament en el desplegament dels objectius tàctics i operatius.**

A la vegada, serà fonamental l'alineament de la funció d'Orquestració Operativa amb els objectius tant tàctics com operatius establerts per cada servei. Per aquest fet, s'hauran d'establir els processos de coordinació necessaris amb els responsables del diferents serveis que composen el AOS, amb l'objectiu de garantir l'alineament homogeni amb els diferents objectius establerts.

- **Generació d'informes i indicadors d'estat de l'Orquestració**

El resultat diari dels focus de treball queda documentat mitjançant el desenvolupament de l'informe de "Fets rellevants", el qual es distribueix diàriament a diferents responsables de l'Agència (via correu electrònic). Serà funció del present servei assegurar que l'informe del "Fets rellevants" inclou informació prou rellevant i de valor, així com garantir que es fa arribar a tots els responsables interns que es defineixin, acomplint els temps i canals acordats.

A la vegada, el licitador haurà d'establir els indicadors necessaris per poder monitoritzar l'activitat generada a partir de l'orquestració, i facilitar la presa de decisions.

2.3.1.2.4 Suport en el seguiment d'objectius estratègics i tàctics

El servei de Governança de l'operativa també és responsable de vetllar per l'assoliment dels objectius estratègics i tàctics de les diferents funcions d'operació de la Ciberseguretat. Per fer-ho, es destaquen les principals tasques a portar a terme:

- Identificar els objectius estratègics i tàctics de l'AOS què pugui definir la Direcció de l'AOS.
- Garantir el desplegament de la estratègia d'operació de la ciberseguretat de l'Agència.
- Vetllar pel correcte càlcul i alimentació de mètriques i indicadors de l'estat de l'operació de ciberseguretat.
- Vetllar per la correcta disposició de quadres de comandament que permetin la visualització del compliment dels objectius i la presa de decisions de manera senzilla i àgil.
- Fer el seguiment periòdic corresponent del nivell d'objectius assolits per identificar i informar amb prou antelació de possibles desviaments o riscos de no compliment d'aquests objectius.
- Promoure la coordinació de tasques entre els serveis operatius de l'AOS per acomplir els objectius definits en els terminis acordats.

2.3.1.2.5 Coordinació davant esdeveniments puntuals de seguretat

Serà funció d'aquest servei actuar com a reforç de les capacitats de gestió dels equips operatius de l'AOS davant situacions puntuals que requereixin d'un seguiment especial o addicional per part de l'àrea d'operacions de seguretat.

A continuació es detallen les accions i funcions principals a desenvolupar per part d'aquest subservei, individualment i de forma transversal, seguint sempre les directrius de la direcció de l'AOS.

De forma individual, per a cada un dels esdeveniments puntals, serien els següents:

- **Operatius de seguretat**

Obtenció i consolidació de la tota la informació de context dels actius a monitorar durant la duració de l'operatiu, incloent l'estat de situació actual de seguretat en base als àmbits de detecció, prevenció, protecció i resposta.

Disseny de l'operatiu de ciberseguretat, incloent:

- Identificació de tots el participants en matèria de ciberseguretat.
- Definició dels requeriments d'operació de la seguretat de forma coordinada amb la resta de serveis operatius de l'AOS i la Direcció de l'Agència.
- Disseny i definició de model de *reporting.*

Coordinació del desplegament de l'operatiu, incloent la interlocució amb les parts definides, i el lideratge del seguiment de l'estat de totes les activitats acordades al disseny de l'operatiu.

Coordinació de l'activació de l'operatiu, assegurant el llançament de les corresponents notificacions, activació dels serveis implicats i acompliment de totes les fites i tasques acordades.

- **Seguiments especials de curta durada**

Obtenció i consolidació de la tota la informació de context dels actius a monitorar durant la duració del seguiment especial, incloent l'estat de situació actual de seguretat en base als àmbits de detecció, prevenció, protecció i resposta.

- Revisió i garantia de la definició d'un model de *reporting*, a mantenir pels equips més operatius implicats en l'execució i seguiment de les tasques durant la duració del seguiment especial.

- Coordinació dels equips operatius de l'AOS per assegurar la correcta execució de les tasques definides durant el seguiment especial.

- **Gestió de crisis:**

Lideratge i coordinació dels aspectes administratius i organitzatius envers la funció de l'operació de la ciberseguretat recollits en l'àmbit d'actuació del servei en els diferents comitès de seguiment/crisis endegats per l'Agència.

Vetllar per la resolució tècnica dels incidents de seguretat crítics i/o d'alt impacte en el negoci, on es compleixin els tres objectius principals: determinar l'afectació/impacte en el negoci, restablir el servei de qualitat el més aviat possible i establir la causa arrel de l'incident.

Definir i implantar metodologies de gestió de crisis amb l'objectiu de millorar el procés i els procediments actuals que s'utilitzen (poca maduresa, ús mínim d'eines definides o poca agilitat).

Registrar i donar visibilitat de forma eficient i amb llenguatge intel·ligible de les accions acordades entre els diferents equips operatius en els comitès de crisis, mitjançant els canals adients per a cada tipologia i que l'Agència determini (per exemple actes de reunió).

Definir i implantar metodologies d'anàlisi en la fase post-crisi, de manera coordinada amb l'equip de resposta a incidents que correspongui i la Direcció de l'Agència, amb l'objectiu de millorar els procediments/eines i aconseguir disminuir el nombre de situacions de crisi futures.

Conèixer i fer ús avançat de les eines implicades en el procés de gestió de crisis, tant les que estiguin vigents en el moment de l'adjudicació del contracte com les que es puguin incorporar durant la vigència del mateix, com a part del servei que presta l'oficina.

- **De forma transversal**:

Participar en la gestió de casos i esdeveniments importants on l'Agència determini que la presència del servei és necessària, donat l'impacte a negoci que pot tenir una potencial amenaça o incident de seguretat.

Establir i implantar procediments de revisió i modificació continus (individuals o globals) sobre la informació/documentació/eines que utilitza el servei per garantir que el servei que en proporciona sigui amb qualitat. Per exemple, disposar de la documentació tècnica i funcional d'un servei actualitzada a la darrera versió o determinar modificacions en la informació emmagatzemada als repositoris actuals.

Proporcionar informes d'incidències sobre els serveis gestionats des de la vessant organitzativa, proposant els canals de comunicació adients per augmentar l'eficiència i l'agilitat extrem a extrem.

Analitzar, de forma continuada, l'execució dels processos de gestió de crisis amb l'objectiu de detectar, proposar i implantar punts de millora en els propis processos, els procediments relacionats i les eines de gestió emprades, en l'àmbit del propi servei o fora del mateix.

Proporcionar informes d'incidències sobre els serveis gestionats des de la vessant organitzativa, proposant els canals de comunicació adients per augmentar l'eficiència i l'agilitat extrem a extrem.

Analitzar, de forma continuada, l'execució dels processos de gestió de crisis amb l'objectiu de detectar, proposar i implantar punts de millora en els propis processos, els procediments relacionats i les eines de gestió emprades, en l'àmbit del propi servei o fora del mateix.

2.3.1.3 Entrega de valor

Un dels reptes que persegueix el AOS, com qualsevol altre servei, és la posada en valor la seva funció dintre de la organització. Actualment, l'AOS disposa d'una estructura molt important, la qual desenvolupa i genera un conjunt molt significatiu d'iniciatives dintre dels diferents àmbits aplicables (Detecció, Protecció, Prevenció i Resposta). Aquestes iniciatives en tot cas permeten a l'Agència assolir els seus objectius, tant operatius, tàctics i estratègics, sent fonamental disposar d'una capa dedicada per poder presentar adequadament els reptes aconseguits i el benefici que representen. Per tot plegat, serà funció del present basat definir, desenvolupar i generar els conjunt de mètriques, indicadors i lliurables que permetin al AOS presentar cap a la Direcció les fites assolides.

Per assolir aquest objectiu serà primordial que el servei disposi d'un coneixement clar de com interactuen i quina activitat generen els serveis del AOS per així aportar una visió integrada i coherent en la construcció i evolució dels indicadors, quadres de comandament i lliurables que generin valor de tota la funció del AOS.

Les principals tasques que haurà de desenvolupar el present servei són:

- Definició de mètriques i indicadors estratègics, alineats amb els objectius de l'Agència, de cadascun dels serveis que composen el AOS.

- Explotar el valor de les principals mètriques i indicadors generats pels equips operatius del AOS de l'Agència, permetent avaluar la consecució dels objectius estratègics de la organització. Aquestes mètriques s'han de poder calcular i consumir mitjançant les eines que es disposen des de l'Agència. Actualment l'eina de presentació d'indicadors utilitzada és Microsoft Power BI.
- Disseny, evolució i millora de quadres de comandament tàctics i estratègics, que permeti disposar per part de la direcció del AOS d'una visió complerta de l'estat dels indicadors dels diferents serveis.
- Coordinació amb els equips tècnics per la implementació del càlcul d'indicadors i desenvolupament dels quadres de comandament definits.
- Suport en la definició de les diferents plantilles de lliurables per presentar el benefici aportat a l'Agència per part dels serveis del AOS.
- Establiment d'un procediment de *reporting* periòdic del valor aportat per les diferents línies de servei a la direcció del AOS.
- Conjuntament amb la direcció del AOS, s'establiran els períodes d'entrega del *reporting* establert, identificant la periodicitat i el contingut dels mateixos. Aquests lliurables hauran de ser desenvolupats pel present servei.

2.3.1.4 Volumetries actuals

Per proporcionar una referència per al correcte dimensionament del servei es proporcionen algunes dades de volumetries observades actualment.

Concepte	Quantitat / any
Casos (tiquets) rebuts i gestionats com a primer nivell del SOC/CERT.	25226
Casos escalats a altres serveis del SOC/CERT (via OTRS)	3262
Casos escalats a tercers fora del SOC/CERT (via Remedy)	5893
Trucades rebudes i gestionades	2690
Revisió de càrrega d'inventaris	12-15
Operatius de seguretat	3
Esdeveniments especials (però sense categoria d'operatiu)	2
Gestió de Comitès de Crisis	47
Lliurables d'entrega de valor d'activitats específiques	11

Durant l'esdeveniment d'operatius de ciberseguretat s'haurà d'estar preparat per assumir l'activitat necessària per atendre a la prestació del servei segons les necessitats pròpies de l'operatiu, tant de capacitat com d'horari, sense que això suposi, en els primers cinc operatius anuals, un cost addicional per l'Agència.

2.3.1.5 Lliurables del servei

El licitador ha de tenir en consideració en el model de prestació del servei, la definició, els continguts i la periodicitat dels lliurables del servei i les seves activitats. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència de Ciberseguretat.

Entre els lliurables es poden considerar productes que inclouen fets rellevants diaris de l'activitat operativa dels serveis, seguiment de l'estat de la demanda registrada a tota l'AOS, resums mensuals i anuals de l'activitat dels serveis, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, notificacions, mètriques i indicadors, entre d'altres.

El llistat que es mostra a continuació, és un mostra dels productes que actualment es lliuren des del servei, indicant la periodicitat definida:

Producte	Periodicitat
Informe de seguiment de l'estat de desplegament de perímetre de sistemes d'informació	Mensual
Informe de seguiment de l'estat de desplegament de perímetre de persones	Mensual
Informe de compliment d'objectius estratègics	Mensual
Informe d'estat de situació del servei	Setmanal
Fets rellevants de l'operativa SOC/CERT	Diari
Memòria anual de l'activitat operativa del SOC/CERT	Quatrimestral
Presentació executiva del valor aportat per una o conjunt d'activitats específiques	Puntual
Informe d'estat de la demanda dels principals serveis del SOC/CERT	Setmanal

La relació de productes de la funció de “Governança de l’operació de l’AOS”, la seva periodicitat i la seva pròpia estructura i continguts s’hauran de definir en la fase inicial abans de la prestació del servei. Aquests podran canviar amb el temps i durant el període d’execució dels serveis que es liciten, d’acord als requisits definits per l’Agència de Ciberseguretat. Els canvis s’acordaran entre l’adjudicatari i la pròpia Agència de Ciberseguretat, garantint no generar un impacte greu en cap de les dues parts.

2.3.1.6 Mètriques i indicadors

Addicionalment als diferents lliurables que pugui generar el servei, aquest també haurà de ser capaç de calcular i facilitar a la capa de “Governança de l’operació de l’AOS”, funció encarregada de la construcció d’indicadors del SOC, totes aquelles mètriques requerides. Previ a fer la petició, s’haurà de definir i analitzar la seva viabilitat, determinant les fonts necessàries i dades necessàries.

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar pel licitador.

Mètrica	Descripció
Coordinació Operativa diària	Nombre d’orquestracions coordinades des del servei.
Comitès de crisi gestionats	Nombre de comitès de crisi gestionats des del servei de amb motiu de la coordinació d’incidents de seguretat.
Sales tècniques gestionades	Nombre de sales tècniques que es gestionen des del servei entre els serveis del SOC i amb l’entitat afectada per
Fets rellevants publicats	Nombre de fets rellevants publicats des del servei
Seguiments Especials coordinats	Nombre de Seguiments Especials coordinats des del servei
Trucades telefòniques ateses	Nombre de trucades telefòniques gestionades des del servei

A més de les llistades per procés, s’hauran de poder obtenir de manera transversal per al servei i l’avaluació dels acords de nivell de servei, com són exemples:

- Nombre de casos/tiquets gestionats pel servei.
- Volum d’hores de dedicació en el servei per cadascun dels membres de l’equip.
- Nombre d'incidències i peticions resoltes segons taula de prioritat en el període.
- Dates d’inici i de lliurament pactat i real de les fites acordades.

- Admissions i desvinculacions de personal de l'equip en el període.

2.3.2 Característiques del servei.

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

L'equip de Governança Operativa de l'AOS haurà de ser transversal, amb capacitats de lideratge i visió tàctica i operativa per garantir la coordinació efectiva entre equips operatius, assegurant l'alineament amb els objectius de l'Agència. Són aspectes clau d'aquest servei la capacitat de supervisió, ordenació i priorització de les tasques operatives, així com la seva capacitat d'adaptabilitat i resiliència a les canviats casuístiques d'un AOS.

Sota un enfocament threat-centric, on l'amenaça és el focus principal que justifica els serveis operatius de l'AOS, aquest servei haurà d'assegurar que totes les activitats de detecció, protecció, prevenció i resposta estiguin enfocades a la priorització i resolució de les necessitats tàctiques derivades del panorama de les ciberamenaces.

Una de les característiques important d'aquest servei es garantir una resposta coordinada, efectiva i eficient davant incidents de ciberseguretat. Per aquest motiu aquest servei haurà de gestionar les comunicacions i els mecanismes necessaris d'activació entre les parts implicades, tant internes com externes, per gestionar adequadament les situacions d'emergència, minimitzant l'impacte sobre l'entitat afectada.

Una altra de les funcions d'aquest servei serà assegurar la consecució dels objectius generals de l'AOS. Per aquest motiu caldrà coordinar operativament els serveis de la mateixa, optimitzant i automatitzant els processos operatius per garantir una resposta ràpida coordinada i eficaç sobre les ciberamenaces i els incidents, proporcionant una visió centralitzada i en temps real de totes les tasques i activitats operatives, mantenint un registre detallat de totes les tasques i accions realitzades i pendents.

Finalment, en l'actualitat aquest servei assumeix un alt nombre de peticions pel que fa a la seva funció de la gestió de la demanda de l'AOS. Caldrà procedir per tant en implantar un procés d'automatització d'aquesta demanda garantint una millor gestió del temps i dels recursos, permetent alhora una resposta mes rapida i precisa davant les necessitats de l'Àrea, que permeti assegurar l'escalabilitat d'aquest servei.

3 Condicions d'execució del servei

3.1 Horaris

El servei de consultoria 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 part caldrà disposar d'un format de guàrdia de 24x7 per tal de fer front als possibles comitès de crisis que puguin aparèixer.

Cal destacar, pel que fa al servei de la gestió de la demanda aquest es realitzarà en prestació de 8:00h fins a les 20:00h en dies laborables

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. Aquestes tasques poden incloure activitats crítiques com ara orquestracions addicionals, operatius especials com poden ser les eleccions o esdeveniments com el Mobile World Congress, o comitès de crisi per fer front a ciberincidents. Sovint, aquestes accions s'han de dur a terme fora de l'horari habitual ja que per la pròpia casuística dels esdeveniments o comitès, es duen a terme fora dels horaris estàndards. Així mateix, i tal i com s'ha esmentat, l'assistència a comitès de crisi també poden requerir intervencions en moments no laborables, especialment en entorns amb alts requeriments de seguretat i continuïtat operativa.

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

3.2 Localització física.

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

Addicionalment, i d'acord amb certes activitats crítiques a les quals aquest servei ha de donar resposta, tal i com s'ha esmentat a l'apartat anterior, s'ha de contemplar la possibilitat que part d'aquests serveis requereixin del desplaçament dels professionals a les instal·lacions dels clients de l'Agència que poden estar ubicades a qualsevol part del territori de Catalunya.

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

3.3 Equip de treball

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

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

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

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

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

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

- El cap de servei és el responsable màxim de garantir que el servei és prestat a l'Agència en les condicions, forma i qualitat pactades i requerides per l'Agència. En cas necessari, el cap de servei haurà d'establir els mecanismes i punts de control per assolir aquest objectiu.
- Garantir la transparència en el control de gestió per tal d'agilitzar el procés de seguiment i facturació.
- Gestió d'altes i baixes del personal de l'adjudicatari conforme els protocols de l'Agència.
- Garantir que els lliurables realitzats s'entreguen a l'Agència en forma i qualitat esperats.
- Coordinar les tasques operatives del servei.
- Reportar al Responsable del Servei de l'Agència els indicadors operatius i de risc del servei.
- Vetllar per la millora continua en els processos i lliurables del servei.
- Gestionar les reunions i els conflictes que puguin aparèixer durant l'execució dels serveis.

Aquesta figura haurà de ser assumida per un membre que alhora compleixi amb un dels perfils de consultor sènior que es descriuen més endavant. És a dir**, no és necessari ofertar un perfil propi de cap de servei/coordinador**, sinó que aquestes funcions s'assignaran a un dels membres mínims requerits.

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

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

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **7.040 hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	Hores anuals mínimes estimades
Consultor Sènior	**3520 hores**
Tècnic demanda	**3520 hores**

3.3.1 Perfils

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

PERFIL	REQUISITS
Consultor Sènior	• Experiència professional mínima de 5 anys en projectes de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Haver participat i poder demostrar la seva involucració en mínim un projecte en els que hagi desenvolupat les següents funcions: ▪ Lideratge de projectes i equips de treball multidisciplinars. ▪ Gestió i operació de serveis de SOC. ▪ Definició de Plans Directors de Seguretat. ▪ Anàlisi de riscos de seguretat i propostes de plans d'acció correctius. ▪ Elaboració d'informes executius, incloent la definició i implantació de quadres de comandament, els quals incorporen visions estratègiques, operatives i tàctiques. ▪ Gestió de projectes de seguretat. ▪ Definició i desplegament de processos de gestió de la seguretat. ▪ Definició, implantació i automatització d'indicadors de servei, especialment en l'àmbit de la ciberseguretat. • Coneixements en: ▪ Definició de projectes (metodologies, processos, eines i lliurables). ▪ Eines de BI, especialment Microsoft PowerBI. ▪ Eines de generació i presentació d'informació per fer més eficient la comunicació i presa de decisions. ▪ Principals vulnerabilitats i defectes a les que poden estar subjectes infraestructures, plataformes i aplicacions (Desbordaments de memòria, Injeccions de codi, errors d'autenticació i autorització, implementacions criptogràfiques incorrectes, gestió deficient d'errors i excepcions, exposició de dades sensibles o configuracions insegures) així com les propostes de mitigació cost/efectivitat més adients. ▪ Principals amenaces i vectors d'atac que afecten a les organitzacions (per exemple, el catàleg d'amenaces que proposa l'organització NIST). ▪ Suport i coordinació en la gestió de crisis i gestió de conflictes

	▪ Suport administratiu en la planificació i formalització d'actes de reunions. Habilitats comunicatives avançades i capacitat de coordinació i interlocució amb altres equips.
Tècnic de suport a la gestió de la demanda	• Experiència professional mínima de 3 anys en l'atenció i gestió de peticions de clients, així com la gestió administrativa i acompanyament a altres funcions en esdeveniments rellevants (p.ex. comitès de crisi). • Titulació en l'àmbit tecnològic actual (incloent formació professional, cicles formatius i altres) que l'habiliti a realitzar les funcions requerides: ▪ Gestió d'eines de tiqueting (OTRS, Jira, Remedy, HP ServiceManager) ▪ Atenció al client ▪ Seguiment administratiu de peticions, formularis i altres tasques relacionades amb la gestió documental. ▪ Interlocució amb equips de treball multi-disciplinar, usuaris clau i usuaris d'alt nivell. • Addicionalment, ha de tenir les següents aptituds mínimes: ▪ Capacitat per l'execució de tasques procedimentades. ▪ Comunicació interpersonal ▪ Lideratge i proactivitat ▪ Habilitats comunicatives i dots de mediació en funció dels destinataris ▪ Capacitat de síntesis ▪ Capacitat d'adaptació ▪ Empatia i alta capacitat d'anàlisi davant situacions crítiques o d'elevada pressió. • Coneixements en: ▪ IT i ciberseguretat bàsica, per facilitar l'atenció i gestió de les peticions responsabilitat del SOC/CERT. ▪ Estàndards com ISO 22320, ISO 22361, per facilitar l'atenció i gestió de situacions de crisis

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.

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.

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 d'infraestructura entre d'altres) per la prestació del servei seran proporcionades per l'Agència. El licitador haurà de fer servir aquestes eines, no podent extreure informació fora de l'àmbit d'actuació per la seva manipulació o explotació sense autorització prèvia de l'Agència.

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

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l'Agència.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides l'Agència.
- Telefonia fixa a les instal·lacions del servei.
- Telefonia mòbil per donar cobertura als serveis de guàrdia.
- Accés a Internet a través de la xarxa d'àrea local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.

L'Agència no proveirà:

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

En conseqüència, els adjudicataris hauran de:

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

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

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

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

3.7 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions com a Centre d'Innovació i Competència en Ciberseguretat (CIC4Cyber) i, especialment, l'impuls de la transformació fonamentada en el coneixement col·laboratiu, la coordinació de l'ecosistema de ciberseguretat i la voluntat per la innovació 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 CIC4Cyber.

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

3.8 Seguretat Corporativa

Un cop adjudicat el contracte basat, tant l'empresa adjudicatària 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:

- 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, i altres regulacions aplicables en matèria de seguretat i protecció de dades).

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, dispositius de xarxa, sistemes operatius i altres elements relacionats), 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, informes d'auditoria i registres de control) 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 estabiran 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, validacions o altres mecanismes de verificació), amb major rigor, intensitat i profunditat segons la cripticitat 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, els recursos necessaris o l'impacte estimat). 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, canvis rellevants en l'entorn tecnològic o riscos identificats), 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.

3.18 Compromís amb el talent femení

El febrer de l'any 2022 l'Agència va aprovar el Pla Estratègic de Dones en Ciberseguretat a l'àmbit de Catalunya, el qual es troba alineat amb les directrius i estratègies impulsades pel Govern de la Generalitat de Catalunya, com ara el Pla Estratègic de Polítiques d'Igualtat de Gènere, l'Estratègia de Ciberseguretat de Catalunya i el Pla Dona TIC, que té com finalitat fomentar la igualtat de gènere en el sector de la Ciberseguretat i, en conseqüència, incrementar el número de dones que es dediquen a la Ciberseguretat. Per deixar palès aquest compromís, i com s'exposa en la memòria justificativa d el'expedient, en aquesta licitació es preveu un criteri d'adjudicació de talent femení.