Plec de prescripcions tècniques particulars que regeix la contractació basada relativa al servei d'arquitectura de seguretat en l'àmbit de la Generalitat de Catalunya,

Exp. CB.24AMCONSL1001

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

2.2.2 Característiques del servei. 7

2.2.2.1 Volumetries orientatives del 2024 9

2.2.2.2 Lliurables del servei 9

3 Condicions d'execució del servei 11

3.1 Horaris 11

3.2 Localització física. 11

3.3 Equip de treball 11

3.3.1 Perfils 13

3.4 Canvi de recurs 15

3.5 Control de rotació 15

3.6 Eines i equipament per a la prestació de serveis. 16

3.7 Gestió del coneixement 17

3.8 Control de Gestió 18

3.9 Documentació. 19

3.10 Formació ..... **Error! No s'ha definit el marcador.**

3.11 Contingència 19

3.12 Metodologia, estàndards i lliurables 19

3.13 Seguretat 19

3.11.1. Deure de confidencialitat 20

3.11.2. Dades de caràcter personal 20

3.11.3. Compliment del marc legal de ciberseguretat i del marc normatiu intern 20

3.11.4. Capacitat tècnica 20

3.11.5. Adquisició de productes/eines i productes o serveis de seguretat 21

3.11.6. Interconnexions 21

3.11.7. Verificació del compliment i auditoria 21

3.11.8. Incidents de seguretat 22

3.11.9. Accés a la informació 22

3.12. Assegurament i control de la qualitat i la millora contínua 22

3.13. Seguiment del servei 23

3.14. Integració amb altres equips 23
3.14 Compromís amb el talent femení 24

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 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.

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 les següents tasques: Suport expert per a la definició de requeriments d'arquitectura de seguretat, identificació, disseny, transformació, homologació i validació d'arquitectures, solucions de seguretat i integració entre solucions les quals son l'objecte de la present licitació.

De totes les àrees que formen l'Agència de Ciberseguretat de Catalunya, l'Àrea d'Operacions 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.

Per dur a terme aquestes funcions, l'àrea d'operacions disposa d'un model de seguretat anomenat perímetre de seguretat. El perímetre de seguretat es defineix com el conjunt d'activitats i tecnologies desplegades i governades pel SOC que contribueixen a la millora de la ciberseguretat dels sistemes d'informació, infraestructures transversals o de les persones.

Els serveis objecte de la present licitació s'emmarquen a la vertical d'evolució i transformació de l'àrea d'operacions. El servei d'Arquitectura de Seguretat defineix, prescriu, evoluciona i valida els models d'arquitectura de seguretat com pot ser el perímetre de seguretat o bé llibres blancs, que defineixen els principis de seguretat que s'han d'implementar en els sistemes TIC en l'àmbit de la Generalitat de Catalunya, així com els projectes i iniciatives d'evolució de la mateixa àrea d'operacions.

2.2 Serveis del contracte Basat

2.2.1 Objecte i abast dels serveis.

L'objecte del present contracte és la contractació de serveis de suport per a la definició, prescripció, evolució i validació dels principis i models d'arquitectura de seguretat per a l'Agència de Ciberseguretat de Catalunya amb la finalitat de millorar la seguretat dels sistemes TIC de les entitats públiques de l'àmbit de la Generalitat de Catalunya i de la pròpia Agència de Ciberseguretat i la possible incorporació d'aquests en el model de protecció que s'ofereix des de l'Agència.

En concret, els objectius que es persegueixen i que es volen assolir amb la contractació d'aquest servei son:

- Definir els models d'arquitectura de seguretat a desplegar en els diferents àmbits que garanteixin el model d'operació de l'Agència i el compliment dels estàndards de seguretat que siguin d'aplicació.

- Evolucionar i avaluar les darreres solucions i tecnologies en l'àmbit de la ciberseguretat per a la seva incorporació en els models d'arquitectura de seguretat.
- Garantir la seguretat des del disseny de nous sistemes d'informació, aplicacions, infraestructures transversals, etc. a través de la prescripció i validació dels principis de seguretat durant la fase disseny de les noves solucions i infraestructures que es construeixin en els diferents àmbits a partir dels models d'arquitectura de seguretat definits.
- Assegurar que els projectes de l'àrea d'operacions compleixen amb els requeriments, models i estàndards en l'àmbit de la seguretat de la informació.

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

Definició dels models d'arquitectura de seguretat

- Construcció, revisió i actualització dels llibres blancs d'arquitectura en base a les diferents especialitats tecnològiques (aplicacions, lloc de treball, infraestructures transversals i identitat digital) i alineat amb els diferents perímetres de seguretat.
- El llibre blanc descriurà els principis rectors de les arquitectures de seguretat de referència i s'anirà detallant en funció de la tecnologia i les solucions concretes.
- Els models d'arquitectura de seguretat hauran de considerar els models d'arquitectura TI establerts en els diferents àmbits.
- Els models d'arquitectura estaran alineats amb els estàndards i normatives que siguin d'aplicació i garantiran el compliment de l'ENS.

Prescripció dels principis d'arquitectura de seguretat

- La prescripció es basarà en el llibre blanc d'arquitectura existent, on es recullen els principis de seguretat a nivell de mesures de protecció, configuracions de seguretat preventives i requeriments que els entorns tecnològics han d'establir.
- S'impulsarà de forma proactiva el desplegament del perímetre adient i el suport per assolir-lo.
- Definir els requeriments de seguretat durant la fase de disseny que les noves solucions hauran d'implementar en funció de la criticitat del sistema d'informació, aplicació, infraestructura, lloc de treball, etc. i de la sensibilitat de les dades que tracti.
- Analitzar i assessorar des d'un punt de vista de la ciberseguretat les arquitectures dels sistemes TIC que es dissenyin.
- Supervisar, durant totes les fases de desplegament, que es duen a terme totes les tasques de ciberseguretat (implantació de mesures, anàlisis tècniques, desplegament de perímetre, gestió de vulnerabilitats, gestió d'excepcions de seguretat).

Evolució i innovació

- Coneixement i seguiment de les tendències del mercat en quant a processos, solucions i tecnologies de ciberseguretat.
- Avaluació i comparació de solucions tecnològiques que puguin donar resposta a necessitats de ciberseguretat identificades.
- Avaluar i actualitzar l'arquitectura existent de l'àrea d'operacions per assegurar que estigui alineada amb les amenaces emergents i les millors pràctiques del sector

2.2.2 Característiques del servei.

De tot el que s'ha exposat prèviament es pot observar com, el servei d'arquitectura té els següents següents elements essencials:

El servei haurà de ser un equip multidisciplinar d'arquitectes de seguretat que, en conjunt, tinguin capacitats i coneixements en aplicacions, sistemes d'informació transversals, infraestructures de lloc de treball, identitat digital, certificats, mecanismes de signatura electrònica, comunicacions, i d'operació de la Ciberseguretat. Siguin aquests en infraestructura de CPD clàssica o al núvol.

També haurà d'assegurar que el disseny de l'arquitectura de seguretat definit per la Generalitat de Catalunya sigui proactiva, eficient i capaç de fer front a un panorama de ciberamenaces en constant evolució. Sota un enfocament threat-centric, cal dissenyar i implementar solucions que prioritzin la detecció, la prevenció i la resposta a les amenaces més crítiques.

El servei d'arquitectura de seguretat haurà de col·laborar amb els equips de l'àrea d'operacions, principalment amb el servei d'evolució i avaluació, per identificar necessitats específiques, com l'adopció de tecnologies emergents (IA, machine learning, entre d'altres), la integració d'intel·ligència d'amenaces i la racionalització dels fluxos de treball. Alhora, el servei d'arquitectura de seguretat establirà les bases tècniques i conceptuals perquè l'àrea d'operacions evolucioni cap a un servei més proactiu, resilient i centrat en l'amenaça, permetent transformar el SOC d'un model reactiu a un model adaptatiu i estratègic, capaç de respondre als reptes actuals i futurs.

El servei haurà de participar en projectes en l'àmbit de la Generalitat de Catalunya, ja siguin impulsats per els Departaments o bé per el CTTI, exercint d'òrgan prescriptor dels requeriments i arquitectures de seguretat. Els projectes poden ser en múltiples entorns tecnològics (aplicacions, sistemes d'informació, sistemes de comunicació, infraestructures de lloc de treball o transversals, identitat digital) ja siguin en infraestructura de CPD clàssica o en el núvol. La prescripció es durà a terme durant la seva fase de disseny o en els exercicis de conceptualització previs. També es validarà els documents de disseny de les solucions i es farà un seguiment durant la fase d'implementació per assegurar que els requeriments i les arquitectures de seguretat queden degudament implementades. Finalment, també es donarà resposta a consultes tècniques relacionades amb la prescripció d'arquitectures de seguretat que es puguin traslladar per part dels departaments i el propi CTTI.

Des del servei, el licitador haurà de ser capaç d'executar els mecanismes adients per tal de fer la integració operativa amb els processos del CTTI (p. ex. obtenció d'informació, consultes a l'inventari d'actius, llançament de peticions i RFC necessàries per a desplegar les mesures de seguretat, aplicació de contramesures, integració amb el Centre de Control, CTTI, identificació d'interlocutors necessaris en els àmbits, integració amb l'equip SAU CTTI...), així com canalitzar les comunicacions necessàries per a les vies i eines establertes.

La funció d'arquitectura de seguretat haurà d'anar més enllà d'un enfocament purament reactiu basat en projectes i consultes rebudes, adoptant una perspectiva proactiva centrada en la identificació de necessitats d'arquitectura encara no establertes i en la detecció d'oportunitats de millora derivades de nous projectes o tecnologies emergents. Aquesta proactivitat implicarà anticipar-se als requeriments de seguretat, proposant solucions innovadores i assegurant que l'arquitectura de seguretat evolucioni per estar alineada amb els objectius de l'Agència de Ciberseguretat i les millors pràctiques del sector de la ciberseguretat.

També s'haurà de tenir en compte processos d'industrialització a l'hora de definir i pensar en els serveis, processos, procediments i eines, i per tant, evitar propostes de serveis que exigeixin: (i) Processos que consumeixin grans esforços de recursos; (ii) Eines amb baix retorn, tant d'eficiència com d'eficàcia; (iii) Processos monolítics i aïllats, que no puguin revertir en millores d'altres processos i serveis, i; (iv) Coneixements tancats, que no comuniquin i que impedeixen el creixement del servei. Tot l'anterior haurà d'estar degudament documentat, demostrant la línia d'industrialització plantejada i tenint en compte quins processos i eines poden ser requerides.

La funció d'arquitectura de seguretat haurà d'incloure la definició de lliurables, especificant-ne el contingut i la periodicitat, amb l'objectiu de garantir que responguin adequadament a les necessitats del servei i contribueixin a millorar-ne tant la prestació com la percepció per part de l'Agència. Aquesta

tasca implica identificar oportunitats per optimitzar la comunicació i els resultats del servei mitjançant documents, informes o altres productes que aportin valor afegit.

Paral·lelament, el servei haurà de millorar i completar les mètriques, productes i lliurables identificats per l'Agència, assegurant que aquests siguin més eficients, rellevants i alineats amb les necessitats del servei. Aquesta tasca implicarà proposar ajustos i ampliacions que augmentin el valor dels resultats lliurats i optimitzin l'acompliment del servei.

2.2.2.1 Volumetries orientatives del 2024

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

Tipologia projecte	Volumetria
Seguretat en disseny d'infraestructures transversals	69
Seguretat en disseny d'aplicacions	257
Seguretat en disseny d'identitat digital	12
Llibres blancs/guies de bones pràctiques	19
Benchmarks / Coneixement de solucions	9
Consultes tècniques	56
Suport d'arquitectura a serveis interns de l'Agència	22

2.2.2.2 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 models de perímetre de seguretat, llibres blancs, presentacions de caire estratègic o tàctic vers l'estat de situació del servei adreçades a la direcció de l' SOC/CERT o la Direcció General de l'ACC, informes de caire evolutiu de caire tecnològic o organitzatiu, resums mensuals i anuals de l'activitat del servei, detall dels incidents/problemes més importants del període, entre d'altres.

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

Producte	Periodicitat
Informe i quadre d'estat del servei	Mensual
Indicadors del servei	Mensual
Informe i quadre de seguiment de les principals tasques i projectes del servei	Setmanal
Documents de llibre blanc o de perímetres de seguretat	Puntual
Document de requeriments de seguretat	Puntual
Fitxa de nova necessitat o document de kick-off d'un nou projecte	Puntual

Informe de benchmark realitzat per part del servei	Puntual
Presentació de conclusions de projecte	Puntual

La relació de productes de la funció, 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.

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. Aquestes tasques poden incloure activitats crítiques com ara l'aplicació de canvis en les arquitectures de seguretat, actualitzacions d'arquitectures de sistemes i dispositius de seguretat (com firewalls, SIEMs o EDRs), analisis de sistemes i infraestructures de resiliència o contingència, o la implementació de mesures de contenció davant d'incidents de seguretat. Sovint, aquestes accions s'han de dur a terme fora de l'horari habitual per evitar interferències amb l'operativa ordinària de l'Agència, minimitzar riscos en serveis productius i garantir la disponibilitat continuada dels sistemes. Així mateix, l'assistència a comitès de crisi o l'ajust d'estratègies de dissenys a arquitectures de seguretat 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, 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, dedicació, pla de treball, etc.) per a l'execució dels serveis sol·licitats en el present plec, d'acord amb les condicions i paràmetres esmentats en els apartats d'aquest plec.

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

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

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

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

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

- Experiència demostrable en desplegament, gestió i direcció de serveis de Ciberseguretat.

Aquesta figura haurà de ser assumida per un membre que alhora compleixi amb un dels perfils d'arquitecte expert que es descriuen més endavant. És a dir, **no s'ha d'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 **8.800 hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	Hores anuals mínimes estimades
Arquitecte de seguretat expert infraestructures transversals	**3520 hores**
Arquitecte de seguretat expert en aplicacions	**3520 hores**
Arquitecte de seguretat expert en identitat digital	**1760 hores**

3.3.1 Perfils

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

PERFIL	REQUISITS

Arquitecte de seguretat Expert infraestructures transversals	• Experiència professional mínima de 5 anys en el món de la seguretat informàtica.
	• Titulació universitària en Enginyeria en informàtica, telecomunicacions o similars en l'àmbit TI.
	• Participació en com a mínim un projecte on hagi desenvolupat les següents funcions:
	  ○ Disseny i desplegament d'infraestructures i solucions de Ciberseguretat.
	  ○ Operació de la ciberseguretat com a part d'un equip SOC/CERT.
	  ○ Gestió de logs en entorns complexes i grans.

	○ Desenvolupament de projectes i sistemes d'informació. • Coneixement en: ○ Governança i definició de millors pràctiques d'arquitectures de seguretat en entorns tant tradicionals com al núvol. ○ Seguretat en els principals protocols de comunicació (TCP/IP, HTTP/S, etc.). ○ Seguretat en entorns IoT i OT. ○ Arquitectures estàndard dels principals fabricants de solucions de ciberseguretat. ○ Tendències tecnològiques, fabricants, estratègies de productes i fulls de ruta. ○ Estàndards i metodologies reconeguts (p.e: ITIL, ISO 27001, PMP, NIST, MITRE ATT&CK, etc.) ○ Sistemes de seguretat tant tradicionals com emergents (Per exemple: WAF, Proxies i Filtrat de continguts, IPS, Firewalls, Routers i switchos, VPN, VRF, sistemes d'encriptació, DNS, DDOS, IPv4 i IPv6, sistemes d'autenticació de múltiple factor, PKI's, DLP, Gestió de logs, sistemes de protecció del lloc de treball, etc).
Arquitecte de seguretat Expert Identitat Digital	• Experiència professional mínima de 5 anys en el món de la seguretat informàtica. • Titulació universitària en Enginyeria en informàtica, telecomunicacions o similars en l'àmbit TI. • Participació en com a mínim un projecte on hagi desenvolupat les següents funcions: ○ Disseny i desplegament de solucions d'identitat digital. ○ Operació i/o administració d'eines de gestió d'identitat o d'accés privilegiat. ○ Projectes en entorns multi-proveïdor. ○ Disseny i/o desplegament de fulls de ruta en aproximacions a ZeroTrust. • Coneixement en: ○ Governança i definició de millors pràctiques d'arquitectures de seguretat en entorns tant tradicionals com al núvol. ○ IAM, IGA, MFA, PAM, KMS, PKI, ID proofing, Autenticació biomètrica, SSI/DCI, ID Wallets, SMCE, Criptografia Post quantum. ○ Coneixement expert en Azure AD, i estàndards SAML, OAuth2, OIDC, SCIM. ○ Estàndards i metodologies corporatives (p.e: ENS, ITIL, ISO 27001, PMP, EIDAS, etc.)

Arquitecte de seguretat Expert Aplicacions	• Experiència professional mínima de 5 anys en el món de la seguretat informàtica.
	• Titulació universitària en Enginyeria en informàtica, telecomunicacions o similars en l'àmbit TI.
	• Participació en com a mínim un projecte on hagi desenvolupat les següents funcions:
	  ○ Disseny i definició de requeriments de seguretat de noves aplicacions.
	  ○ Analisi i validació de la seguretat d'arquitectures de sistemes d'informació.
	  ○ Disseny i evolució dels processos de seguretat dins el cicle de vida del desenvolupament d'aplicacions
	• Coneixement en:
	  ○ Governança i definició de millors pràctiques d'arquitectures de seguretat de sistemes d'informació, tant tradicionals com al núvol
	  ○ Metodologies de desenvolupament i gestió de projectes de software, en especial DevSecOps
	  ○ Processos i eines d'anàlisis tècniques de seguretat i gestió de vulnerabilitats
	  ○ Estàndards i normatives (ENS, ISO27001, ...)

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. Si l'objecte del contracte basat ho requereix, aquest aspecte es podrà concretar en el contracte basat.

3.6 Eines i equipament per a la prestació de serveis.

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

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

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

L'Agència no proveirà:

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

En conseqüència, els adjudicataris hauran de:

- Subministrar tots elements de maquinari, programari i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments de l'objecte del contracte. Aquests elements seran ***d'ús exclusiu*** pels serveis prestats a l'Agència i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.

- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.
- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip de Mitjans Tècnics de l'Agència.

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

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

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

3.7 Gestió del coneixement

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

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.
- 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.

3.8 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.

3.9 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

3.10 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.

3.11 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.

3.12 Seguretat

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

3.11.1. Deure de confidencialitat

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

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

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

3.11.2. Dades de caràcter personal

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

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

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

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

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

3.11.4. Capacitat tècnica

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

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

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

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

L'empresa adjudicatària del contracte basat haurà de garantir que disposa dels perfils amb la 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.

3.11.6. Interconnexions

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

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

3.11.7. Verificació del compliment i auditoria

L'Agència es reserva el dret a verificar i auditar, amb mitjans propis o de tercers, el compliment de les mesures de seguretat requerides en base al marc legal de ciberseguretat i al marc intern per als sistemes d'informació emprats per a l'execució del contracte, en el moment i amb la periodicitat que s'estimi convenient. L'Agència podrà requerir el seguiment dels plans d'acció derivats d'aquestes verificacions i auditories. L'empresa adjudicatària del contracte basat haurà de disposar dels

recursos adients per a dur terme l'execució de les tasques que li corresponguin en relació a aquest model de compliment, donant resposta en els terminis marcats per l'Agència de Ciberseguretat. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència de Ciberseguretat.

3.11.8. Incidents de seguretat

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

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

3.11.9. Accés a la informació

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

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

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

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

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

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

3.13. Seguiment del servei

Les empreses adjudicatària haurà de presentar un informe de seguiment. Aquests informes s'avaluaran als comitès operatius i es formalitzaran i s'elevaran els seus resultats a la resta de comitès.

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

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

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

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

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

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

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

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

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

3.14. Integració amb altres equips

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

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

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

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

3.13 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.

En virtut de l'anterior, i com s'exposa i justifica en la Memòria Justificativa del present expedient, s'inclou un criteri de valoració referent al foment del talent femení.