Plec de prescripcions tècniques particulars que regeix la contractació basada relativa als serveis de suport a les funcions pròpies de l'àrea d'Estratègia d'àmbits en l'àmbit Salut, estructurada en 3 lots

Lot 1: Suport a la Coordinació del model de Ciberseguretat seguretat a l'àmbit hospitalari, primària, sociosanitari (intermèdia) i salut mental.

Lot 2: Suport al seguiment dels plans de seguretat a l'àmbit hospitalari i primària

Lot 3: Suport al seguiment dels plans de seguretat a l'àmbit sociosanitari (intermèdia) i salut mental

Exp. CB25AMCONSL1B010

Índex

1. Introducció

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència), establerta sota el marc de la Llei 15/2017, del 25 de juliol, és l'entitat que lidera i coordina els esforços de la Generalitat de Catalunya en la protecció de la informació i les infraestructures del país davant les ciberamenaces. En un món digitalitzat i interconnectat, la seguretat de la informació s'ha convertit en una prioritat estratègica, i l'Agència subratlla el compromís de Catalunya amb la promoció d'un entorn digital segur i de confiança. Dins d'aquest context, els acords marc en matèria de ciberseguretat representen una eina essencial per a la implementació de solucions i serveis que reforcin la ciberseguretat de Catalunya, alineats amb l'Estratègia de Ciberseguretat 2019-2022 i la proposta per a la nova Estratègia 2023-2027.

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

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

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

En el marc de l'activitat gestionada per l'Agència de Ciberseguretat, cal destacar que aquesta gestiona més de 2.200 sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants. Aquest perímetre protegit provoca un nivell d'activitat de gestió de més de 4.424 milions de ciberatacs durant el 2022, una xifra 20 cops superiors a la del 2021.

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

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

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

Avui en dia l'Agència té les següents funcions:

- L'Àrea de Gerència s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació i la gestió de personal.
- Operació de la Seguretat du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció, resposta i recuperació de seguretat en la seva vessant més operativa i la seguretat corporativa.
- Desenvolupament d'Estratègia d'Àmbits té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes i iniciatives de seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- Producte i Centres de Competència i Innovació (DIP) s'ocupa, per una banda, d'identificar les necessitats i proposar noves idees i estratègies per a l'elaboració de nous productes generats per l'Agència o millora dels existents, i coordina l'execució del cicle de vida dels productes, des de la seva concepció fins a la seva retirada, incloent el disseny, desenvolupament, desplegament i control de qualitat. Per una altra banda, coordina, cohesiona i capacita l'ecosistema de la Ciberseguretat de Catalunya, recolzant el coneixement, sensibilització i conscienciació com a palanca de la transformació i creixement del sector
- 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. Antecedents

Els estudis de tendències constaten que els atacs cibernètics a centres sanitaris poden provocar greus impactes en la qualitat assistencial als pacients, poden impedir l'accés als expedients mèdics i bloquejar el funcionament de tots sistemes informàtics, i per tant, provocar retards en els procediments i proves, i hospitalitzacions més llargues.

En aquest context, l'Agència de Ciberseguretat va detectar més de mil milions d'atacs dirigits contra el sector sanitari a Catalunya durant el 2023, dels quals 308 van materialitzar-se en incidents. Alguns d'ells, com els succeïts a l'hospital Clínic o al Moises Broggi (Consorci Sanitari Integral) van suposar un greu impacte assistencial per la ciutadania, ja que van afectar de forma directa als principals hospitals i centres d'atenció primària del nucli de Barcelona.

Davant d'aquesta situació l'Agència de Ciberseguretat en el 2023 va accelerar el desplegament del Model integral de Ciberseguretat (en endavant, el Model), que té com a objectiu protegir els àmbits d'actuació públics més rellevants a Catalunya de les amenaces en ciberseguretat dirigides contra els seus sectors, i abordar les actuacions necessàries per a protegir-los dels ciberincidents que puguin impactar contra les diferents entitats que els conformen.

Aquest model consta de tres primeres fases de Desplegament (Diagnòstic, Pla de Seguretat i Integració) i dues més, de serveis recurrents i certificació en l'ENS.

- **Diagnòstic:** identificació del grau actual d'exposició a les principals ciberamenaces que apliquen a l'àmbit.
- **Pla de seguretat:** determinació del pla de seguretat de cada entitat per tal de ser més resilient i reduir l'exposició a les amenaces més significatives, amb una orientació a assolir el compliment normatiu en l'Esquema Nacional de Seguretat i, quan correspongui, en altres normatives sectorials o específiques que siguin d'aplicació.
- **Integració operativa:** desplegament, a partir de les capacitats de protecció desplegades per les entitats, de les capacitats de prevenció, detecció i resposta, i dels processos i serveis associats a la integració amb l'Agència de Ciberseguretat de Catalunya.
- **Serveis recurrents:** activació i operació del serveis de monitorització i resposta 24x7 de l'Agència, i dels serveis necessaris per a la governança, comunicació, formació i evolució en la ciberseguretat.
- **Certificació en l'ENS:** procés de certificació mitjançant les auditories de la conformitat en l'Esquema Nacional de Seguretat.

A inicis del 2024 es donen per finalitzades les tasques pròpiament de desplegament a les entitats proveïdores d'atenció especialitzada del SISCAT (sistema sanitari integral d'utilització pública de Catalunya) i es posen en marxa els serveis recurrents. Durant el 2024 aquest model, desplegat i en ple funcionament a través dels serveis recurrents, va permetre detectar un total de 1257 milions d'atacs i gestionar més de 676 incidents de seguretat amb les entitats sanitàries (dades extretes de la memòria de l'Agència del 2024)

Donada la interconnexió existent a tot l'àmbit de Salut, no només entre els centres hospitalaris del SISCAT, sinó també amb i entre els centres sociosanitaris, centres de salut mental i atenció primària, es preveu fer extensiu durant el 2025 i 2026 el desplegament del model a la resta de línies assistencials esmentades, amb l'objectiu de generar una protecció homogènia, conjunta i coordinada. Aquest desplegament, previst durant els anys 2025 i 2026, donarà pas als serveis recurrents amb l'objectiu de garantir un procés de millora continua i per tant un increment de la seguretat del servei públic de salut de Catalunya.

Per a materialitzar tot l'anterior, el Servei Català de la Salut i l'Agència de Ciberseguretat de Catalunya van signar la sol·licitud d'actuació SOC-5100-25-003 en el marc del Contracte Programa de l'Agència de Ciberseguretat de l'Agència 2024-2027, el qual ha estat aprovat per Acord de Govern de 8 d'abril de 2025, en el que s'aproven les despeses amb càrrec a pressupostos d'exercicis futurs, per un import total de 27.000.000,00 euros, per al finançament de determinades actuacions de Ciberseguretat sobre el SISCAT.

L'objectiu de dita petició és la realització d'actuacions de Ciberseguretat relacionades amb el desplegament i consolidació del Model de Ciberseguretat a les entitats proveïdores del SISCAT incloent les 3 línies assistencials: atenció especialitzada o hospitalària, sociosanitaris (intermèdia) i salut mental, i atenció primària per tal de millorar la resiliència i les capacitats de protecció, prevenció, detecció i resposta en matèria de Ciberseguretat del sistema sanitari públic de Catalunya (SISCAT) així com avançar cap a la certificació en l'Esquema Nacional de Seguretat (ENS).

2.1. Objectius generals del model i dels serveis de suport objecte de la licitació

Els objectius generals del Model Integral de Ciberseguretat, desplegat en les entitats del SISCAT, i objecte de la present licitació, per al servei de suport **a l'Agència en el seguiment i evolució en ciberseguretat** de les entitats del **SISCAT** són:

- **Vetllar i donar suport a l'Agència en el seguiment de les entitats per al progrés i millora continua en Ciberseguretat**.
- **Donar suport en el seguiment del progrés i l'execució dels Plans de Seguretat** de les entitats del SISCAT, de manera homogènia, coordinada i traçable.
- **Col·laborar en l'impuls de l'estratègia d'adequació i certificació a l'ENS**, proporcionant guiatge, criteris, eines i suport a les entitats per avançar en el compliment i la certificació.
- Proporcionar **assessorament especialitzat i proactiu** en matèria de seguretat de la informació, vetllant per la correcta sincronització dels diferents serveis del model.
- Donar suport a l'Agència en la millora del Model i els serveis prestats a les entitats, a través de la recollida i anàlisis periòdic del feedback de les entitats.
- Reforçar a l'Agència en les funcions de **coordinació** de les entitats de les diferents línies assistencials i en la interlocució amb els diferents serveis recurrents del Model (prevenció, detecció, resposta, formació, innovació, govern de la dada, arquitectura, etc.), vetllant per la **interoperabilitat operativa** dels diferents serveis del model i una execució coordinada i alineada.
- Assistir les tasques de **reporting del Model de la proposta i generació d'indicadors** periòdics així com proposar **mecanismes de millora contínua**, per reforçar l'excel·lència operativa i l'evolució sostinguda de la maduresa en ciberseguretat de l'àmbit de Salut. Els destinataris d'aquests indicadors seran el Departament de Salut, l'Agència de Ciberseguretat i les mateixes entitats.

3. Descripció dels serveis objecte de la contractació basada.

3.1. Context dels serveis objecte de la licitació i abast

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.

Dins de dit lot s'inclouen les actuacions que s'enumeren en els següents apartats, les quals són plenament assimilables a l'objecte de la present licitació.

L'Agència té com a objectiu mitjançant el present basat de dotar-se de les capacitats necessàries per al suport del seguiment i evolució en ciberseguretat de les diferents de les entitats del SISCAT integrades en el Model Integral de Ciberseguretat així com la millora del model i dels serveis recurrents que el conformen.

En aquest sentit, i a mode de referència, les entitats del SISCAT incloses en el Model de Ciberseguretat i per tant incloses en l'abast, són les següents :

- **68 entitats d'atenció especialitzada o hospitalària**: model desplegat i operant en serveis recurrents des del 2024
- **93 entitats sociosanitàries (intermèdia) i salut mental**: incorporació progressiva al Model durant **2025 i 2026**
- **Mes de 400 centres d'atenció primària**: integració amb una visió inicialment més tecnològica (incloent eines de protecció perimetral), dels quals aproximadament un 75% són proveïts i gestionats per l'Institut Català de la Salut (ICS).

Cal tenir en compte que, algunes entitats no presten només servei en una línia assistencial, sinó a vàries. Això, juntament amb el fet que algunes entitats poden tenir infraestructura tecnològica compartida, implica que alguns centres es gestionin de forma conjunta, unificant interlocutors i serveis.

En el següent enllaç es pot obtenir informació addicional del model desplegat: https://salutweb.gencat.cat/ca/ambits-actuacio/linies/tic/governanca-innovacio-seguretat/model-integral-ciberseguretat-sector-sanitari/.

En funció d'aquest abast, i de les necessitats de suport derivades del desplegament del model, el present basat ha estat distribuït en els següents 3 lots:

- Lot 1: Suport a la Coordinació del model de Ciberseguretat seguretat a l'àmbit hospitalari, primària, sociosanitari (intermèdia) i salut mental.
- Lot 2: Suport al seguiment dels plans de seguretat a l'àmbit hospitalari i primària
- Lot 3: Suport al seguiment dels plans de seguretat a l'àmbit sociosanitari (intermèdia) i salut mental

4. Lot 1: Suport a la Coordinació del model de Ciberseguretat seguretat a l'àmbit hospitalari, primària, sociosanitari (intermèdia) i salut mental.

L'objecte d'aquest Lot és el suport a les funcions de l'Agència associades al seguiment i evolució del Model de Protecció de l'Agència, així com a les tasques de coordinació i gestió associades, ambles entitats proveïdores del SISCAT de a les línies assistencials d'atenció especialitzada (u hospitalària), sociosanitària i salut mental, i primària.

4.1.1. Objectius del servei

L'objectiu principal d'aquest lot és donar suport a l'Agència en la coordinació de les diferents línies assistencials que formen part del model: atenció especialitzada o hospitalària, primària, atenció sociosanitària i salut mental. Les funcions de suport que es descriuen van orientades vetllar per una gestió homogènia i coordinada de les 3 línies però tenint en compte les particularitats de cadascuna d'elles. Per aquesta raó moltes de les funcions descrites en tracten a nivell global d'àmbit salut, però també a nivell de línia assistencial. Aquest lot treballarà en coordinació i amb els Lots 2 i 3 d'aquest plec per ajudar en l'agregació d'informació que facilitin a l'Agència de presa decisions.

Així mateix, el servei assistirà a l'Agència en el seguiment de l'execució de les activitats previstes en temps i forma, vinculades al Model Integral de Ciberseguretat, i d'acord amb les directrius establertes per la Direcció d'Estratègia d'Àmbits de Salut (en endavant DEA Salut).

Qualsevol situació de risc detectada, ja sigui en relació als serveis recurrents del model, amb alguna entitat concreta o línia assistencial, serà degudament identificada i traslladada a DEA Salut perquè aquesta pugui activar els mecanismes corresponents, tant en l'àmbit operatiu com amb les àrees internes que escaigui, per abordar i readreçar la situació.

4.1.1. Volumetries previstes

L'abast del projecte i les volumetries que es contemplen en el Lot 1 són les següents:

- **68 entitats d'atenció especialitzada o hospitalària del SISCAT**, amb el model desplegat i operatiu des del 2024.
- **93 entitats d'atenció sociosanitària (intermèdia) i de salut mental** que s'incorporen al model durant el 2025 i 2026.
- **més de 400 centres d'atenció primària del SISCAT**, dels quals aproximadament un 75% són proveïts i gestionats per l'Institut Català de la Salut (ICS).

Aquest volum és una estimació i com a tal podrà ser ajustat per l'Agència en funció de l'evolució del desplegament i de les necessitats operatives que es determinin durant la vigència del contracte.

4.1.2. Finalitat i funcions del servei

Els serveis inclosos en aquest Lot 1 tenen com a finalitat donar suport al seguiment i evolució de la maduresa en ciberseguretat de les entitats del SISCAT integrades en el Model Integral de Ciberseguretat impulsat per l'Agència de Ciberseguretat de Catalunya, així com a les tasques de coordinació i gestió associades.

En aquest sentit, entenem per **suport a la coordinació i gestió,** l'execució de les següents funcions:

- **Suport al seguiment del model de forma global** per garantir el progrés sostingut de les diferents línies assistencials: hospitalària, primària, sociosanitaris i salut mental.
- **Col·laboració** amb l'Agència en la **recollida de la informació rellevant** de les entitats, per generar **un coneixement agregat de l'àmbit de salut i de les diferents línies assistencials. Unificació del coneixement** de l'àmbit, **identificació de riscos**, problemàtiques comuns i proposta de possibles solucions i/o projectes per abordar-les.
- **Vetllar conjuntament amb l'Agència per al seu progrés i evolució en Ciberseguretat** a través de l'assessorament expert i l'acció coordinada amb la resta de serveis del Model.
- **Participació i assessorament en identificació de problemàtiques** comunes i proposta de possibles solucions o projectes.
- **Col·laboració en l'alineament dels missatges clau** dirigits a les entitats per assegurar la coordinació global de tot el model.
- **Suport en el seguiment global** del desplegament dels diferents projectes i iniciatives de Ciberseguretat que deriven dels plans de seguretat per la millora de la maduresa global de l'àmbit i les diferents línies assistencials.
- Suport en la generació de propostes i estratègies per a l'impuls en l'adequació i certificació en l'ENS.
- **Suport a la coordinació i planificació** de les actuacions necessàries derivades d'altres serveis recurrents del Model i alineades a les particularitats de les diferents línies assistencials.
- **Comunicació propera i proactiva** amb les entitats.
- Participació en la generació de propostes per a l'impuls en la coordinació i la interoperabilitat operativa amb la resta de capacitats i serveis recurrents del Model (prevenció, detecció, resposta 24x7, arquitectura, govern de la dada, formació, innovació, comunicació i altres), buscant sinèrgies i coordinació amb les entitats.
- Proposta d'eines de gestió de la documentació amb les entitats i de forma coordinada amb seguretat corporativa de l'Agència.
- Ajudar a l'Agència en la gestió coordinada i homogènia dels lots 2 i 3 d'aquesta licitació.
- Suport en la orientació dels lots 2 i 3 per assegurar el bon funcionament sobretot en les fases inicials a través de l'acompanyament a kick-offs, presentacions de resultats, etc.
- Col·laboració en la revisió de la qualitat dels entregables del propi lot de coordinació i dels entregables dels lots 2 i 3 per garantir una qualitat homogènia per totes les entitats i sota els mateixos criteris.
- Col·laboració en la **generació d'indicadors globals d'àmbit,** per a les diferents **línies assistencials i a nivell particular de les entitats,** amb l'objectiu de seguir la maduresa en ciberseguretat i la seva evolució. És important evidenciar l'evolució de la Ciberseguretat a l'àmbit de Salut, així com l'impacte global del model.
- Generació **d'indicadors generals del servei i específics per al reporting** quan escaigui.
- Col·laboració i transferència de coneixement de les dades generades des del servei a l'àrea de Govern de la dada de l'Agència per la seva representació.

- **Suport a la preparació de reunions i informes** per al seguiment del projecte amb la Coordinació General de les TIC del Departament de Salut i el Servei Català de la Salut (CATSALUT).
- **Recolzament en la preparació i participació**, si escau, en **les reunions** amb altres entitats (més enllà de les entitats proveïdores del SISCAT i el Departament de Salut). Alguns exemples són: Comitè Estratègic de Ciberseguretat al Departament de Salut, patronals de Salut, Institut Català de la Salut (ICs), CTTI, etc.
- Identificació d'accions de millora que permetin **l'evolució del model i/o dels seus serveis**.
- **Identificar i aixecar riscos** en l'execució dels serveis.
- Ús de les eines de reporting i seguiment pròpies de l'Agència i de forma coordinada amb les àrees internes de l'agencia i seguint les seves indicacions per a la correcte planificació i facturació de l'activitat del lot.

4.1.3. Lliurables i mètriques del servei

En el marc del Lot 1, l'adjudicatari haurà de **donar suport a l'Agència en les tasques de revisió, harmonització i unificació dels lliurables generats pels Lots 2 i 3**, d'acord amb les directrius, criteris metodològics i instruccions que l'Agència determini en cada moment. Aquesta funció té per finalitat assegurar que tots els lliurables del servei presentin un nivell homogeni de qualitat, coherència tècnica i alineament amb el Model de Ciberseguretat impulsat per l'Agència.

S'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.

Molts d'aquests lliurables es generen a través de l'agregació i anàlisi dels lliurables individuals d'entitats generats en els lots 2 i 3. Amb aquesta agregació es genera un visió més global de tot l'àmbit sa Salut i per línies assistencials i això afavoreix la presa de decisions i propostes de millora.

A nivell orientatiu en l'execució del servei es demanaran els següents lliurables de seguiment del servei:

Lliurable	Descripció	Freqüència
Pla de Coordinació Global	Estratègia, calendarització i circuits de coordinació amb totes les línies assistencials i serveis recurrents.	Inicial + actualització anual
Informe Mensual d'evolució del Model	Seguiment agregat del progrés dels plans de seguretat i el progrés en l'Esquema Nacional de Seguretat i per línies assistencials; riscos, desviacions i decisions de coordinació amb l'Agència.	Mensual
Actes de reunions de Coordinació Transversal	Actes, acords, tasques, bloquejos i decisions.	Després de cada reunió

Document de Coordinació amb Serveis Recurrents	Seguiment d'interdependències i activitat amb serveis transversals del Model.	Mensual
Context global de les entitats	Informació de context de les entitats rellevant, agregada de forma global i per línies assistencials.	Mensual
Estat dels Plans de seguretat	Identificació d'iniciatives i accions que evolucionen més ràpidament i més lentament per part de les entitats.	Trimestral
Estat dels Perímetres	Evolució en el temps de les funcionalitats dels perímetres global i per línies assistencials. Recull d'eines emprades per al perímetre.	Trimestral
Full agregat de les activitats planificades amb les entitats	Registre complet d'activitats planificades, executades i pendents, de forma global i per línies assistencials. P.ex: formacions, simulacres, etc.	Mensual
Informe de desviacions i incidències	Resum agregat d'incidències i desviacions detectades. Identificació d'incidències recurrents.	Mensual
Informe de la situació global de les entitats i per serveis	Resum de la situació actual global i per línies assistencials a través de la informació dels informes individuals de situació de les entitats. Resum de situació per serveis. Anàlisis de la informació recollida per entitats i identificació de paràmetres interessants d'agregar per facilitar l'evolució de les entitats o per identificar situacions per permetin la presa de decisions amb els responsables de l'Agència.	Trimestral o sota demanda
Registre de Riscos operatius d'Entitat	Identificació de situacions de risc amb les entitats i mesures correctores proposades	Mensual
Enquesta de Satisfacció	Puntuacions agregades de les enquestes de satisfacció del model amb les entitats a nivell global i per línies assistencials	Anual
Informe Anual del Model de Ciberseguretat	Mostra de la evolució anual agregada anual de global i per línies assistencials a través dels informes individuals. Anàlisi global de resultats, maduresa assolida i propostes de millora.	Anual

Quadre de Control Trimestral del Model	Dashboard complet d'indicadors del Model: KPIs, riscos, evolució	Trimestral

Amb la finalitat de donar suport a l'Agència en el seguiment, control i avaluació de la prestació del servei, s'haurà de preveure i garantir la generació de, com a mínim, les mètriques que s'indiquen a continuació.

Mètriques	Descripció
Nombre d'entitats en seguiment	Estat agregat a nivell de volumetries de les entitats integrades i en seguiment: especialitzada, primària, sociosanitària i salut mental.
Activitats globals, segregades i individuals	Activitats executades dins del lot de forma global, per línies assistencials i per entitat, si escau. Indicació d'activitats dutes a terme i fites assolides.
Actualitzacions efectuades	Nombre d'actualitzacions de la informació de context de les entitats (contactes, perímetre, ec) a nivell global i per línies assistencials.
Consultes derivades a d'altres serveis del Model	Consultes derivades i resoltes a través d'altres serveis del Model.
Controls avaluats	Nombre de controls avaluats globals i per línies assistencials.
Lliurables generats	Nombre de lliurables generats i entregats.
Seguiments realitzats	Nombre de reunions de seguiment internes dels equips i de punts de control amb l'Agència. Nombre de reunions efectuades amb els Lots 2 i 3.
Informe Anual del Model de Ciberseguretat	Anàlisi global de resultats, maduresa assolida i propostes de millora.

Addicionalment al disposat al quadres anteriors, i en el marc del principi de millora contínua del servei, l'Agència podrà requerir l'elaboració de nous lliurables i mètriques addicionals als ja definits, sempre que aquests resultin necessaris per garantir una execució eficient, homogènia i plenament alineada amb les necessitats operatives del Model i estiguin relacionats amb l'objecte del contracte.

5. Lot 2: Suport al seguiment dels plans de seguretat a l'atenció hospitalària i primària

L'objecte d'aquest lot és el suport al seguiment dels Plans de Seguretat de les entitats del Model de Ciberseguretat de l'atenció hospitalària i primària.

5.1.1. Objectius del servei

L'objectiu principal d'aquest lot és donar suport a l'Agència en la interlocució i l'acompanyament de les entitats, mitjançant la recopilació sistemàtica de la informació de context necessària per facilitar-ne un assessorament adequat i garantir el correcte progrés de les seves actuacions en matèria de ciberseguretat. Així mateix, el servei assistirà l'Agència en la correcta execució de les activitats vinculades al Model de Ciberseguretat, d'acord amb les directrius establertes per la Direcció d'Estratègia d'Àmbits de Salut (DEA Salut).

El personal assignat actuarà com a punt de suport expert, participant en les activitats que involucrin les entitats amb l'objectiu d'aportar criteri tècnic, elevar les consultes que escaiguin als òrgans competents de l'Agència i garantir la traçabilitat de les qüestions plantejades. Igualment, qualsevol situació de risc detectada en relació amb una entitat serà degudament identificada i traslladada a l'Agència perquè aquesta pugui activar els mecanismes corresponents, tant en l'àmbit operatiu com en les àrees internes que escaiguin.

5.1.2. Volumetries previstes

D'acord amb l'abast funcional del servei i amb les necessitats de suport identificades per l'Agència, aquest lot prestarà assistència tècnica en el seguiment **68 entitats de l'àmbit d'atenció especialitzada** o hospitalària i més de **400 centres d'atenció primària**, integrats en el Model de Ciberseguretat del SISCAT. Del total de centres d'atenció primària aproximadament un 75% són proveïts i gestionats per l'Institut Català de la Salut (ICS)

Aquest volum és una estimació i com a tal podrà ser ajustat per l'Agència en funció de l'evolució del desplegament i de les necessitats operatives que es determinin durant la vigència del contracte.

5.1.3. Funcions i activitats del servei

El servei inclou les tasques següents per al seguiment dels Plans de Seguretat amb les entitats del SISCAT:

- **Donar suport a l'Agència en la interlocució amb les entitats**, contribuint al coneixement del seu context i a la vigilància del seu progrés en matèria de ciberseguretat mitjançant assessorament expert i d'acord amb les directrius establertes per l'Agència.
- **Assistir a l'Agència en la revisió dels avenços, activitats, riscos, desviacions i necessitats** plantejades per les entitats, mitjançant la interlocució operativa que es determini en cada cas.

- **Donar suport al seguiment operatiu dels Plans de Seguretat** de les entitats assignades, en coherència amb els criteris i pautes definits per l'Agència.
- **Elaborar, recollir i consolidar els indicadors establerts pel Model**, aportant la informació requerida per a l'anàlisi i la presa de decisions per part de l'Agència.
- **Acompanyar l'Agència en reunions, activitats de revisió documental i suport a la implementació de mesures de seguretat**, actuant sempre com a assistència tècnica i no com a òrgan decisori.
- **Col·laborar amb la resta de serveis recurrents del Model**, d'acord amb les instruccions de l'Agència.
- **Donar suport en la gestió de dubtes de seguretat plantejats per les entitats**, incloent la seva tramitació, seguiment i tancament sota la supervisió de l'Agència.
- **Assistir en l'elaboració de documentació i plantilles** per al treball amb les entitats, d'acord amb els formats, criteris i procediments establerts per l'Agència.
- **Acompanyar les entitats en els seus processos de certificació i auditoria**, proporcionant assessorament i suport tècnic conforme a les indicacions de l'Agència.
- **Donar suport continu a les entitats** en presentacions, activitats i accions derivades de la interacció amb la resta de serveis del Model.
- **Proporcionar assistència en la interlocució amb altres serveis de l'Agència**, quan així es requereixi.
- **Generar informes d'estat de les entitats amb la periodicitat establerta** per l'Agència, ajustant-se a les instruccions de contingut, format i circuit de validació.
- **Utilitzar les eines de reporting i seguiment pròpies de l'Agència**, treballant de manera alineada amb les àrees internes per garantir la correcta planificació i facturació de les activitats del lot.
- **Donar suport a l'Agència en la interlocució amb entitats que requereixin una visió agregada**, com en el cas de l'Institut Català de la Salut (ICS), facilitant el tractament conjunt de la informació i el seguiment coordinat amb les seves gerències.

5.1.4. Lliurables i mètriques del servei

S'haurà de preveure i garantir la generació, com a mínim, dels lliurables que s'indiquen a continuació.

Lliurable	Descripció	Freqüència
Context de l'entitat	Documentació que reculli tota la informació de context recopilada de cada entitat per al coneixement com a referent de la mateixa	Puntual a l'inici i quan es produeixin actualitzacions
Informe de Seguiment per Entitat	Estat del pla de seguretat, activitats, desviacions, riscos i necessitats.	Trimestral
Estat dels Plans de seguretat	Evolució en el temps dels plans de seguretat per cadascuna de les entitats.	Trimestral
Estat dels Perímetres	Evolució en el temps de les funcionalitats dels perímetres per entitat. Recull d'eines emprades per al perímetre.	Trimestral

Full d'activitats amb les entitats	Registre complet d'activitats executades i pendents per entitat a nivell de formació, simulacres, etc.	Mensual
Actes de reunions amb entitats	Acords, tasques i calendaris de les reunions amb cada entitat.	Després de cada reunió
Informe de desviacions i incidències	Resum dels incidents i desviacions detectades durant el seguiment.	Mensual
Informe de la situació actual d'una entitat	Resum de la situació actual per entitat.	Trimestral o semestral
Registre de Riscos Operatius d'Entitat	Identificació de situacions de risc amb les entitats i mesures correctores proposades	Mensual
Informe de situació anual	Mostra de la evolució anual agregada anual de l'entitat.	Anual

Amb la finalitat de donar suport a l'Agència en el seguiment, control i avaluació de la prestació del servei, s'haurà de preveure i garantir la generació de, com a mínim, les mètriques que s'indiquen a continuació.

Mètriques	Descripció
Nombre d'entitats en seguiment	Estat agregat del conjunt d'entitats assignades i en seguiment: especialitzada i primària.
Activitats amb les diferents entitats	Nombre de reunions de seguiment efectuades amb les entitats. Agregació per línies assistencials.
Activitats globals, segregades i individuals	Activitats executades dins del lot de forma global, per línies assistencials i per entitat. Indicació d'activitats dutes a terme i fites assolides.
Actualitzacions	Actualitzacions de la informació de context de les entitats: contactes, perímetre, etc.
Consultes	Consultes derivades i resoltes a través d'altres serveis del Model. Per exemple: - Consultes derivades cap a gestió de l'àmbit de Salut del SOC. - Consultes derivades cap a arquitectura.
Controls avaluats	Nombre de controls avaluats per cada entitat i de forma acumulada.
Lliurables generats	Nombre de lliurables generats i entregats.

Seguiments realitzats	Nombre de reunions de seguiment internes dels equips i de punts de control amb l'Agència.
Enquesta de Satisfacció	Puntuacions de les enquestes de satisfacció del model amb les entitats.
Informe Anual del Model de Ciberseguretat	Anàlisi global de resultats, maduresa assolida i propostes de millora.

Addicionalment al disposat als quadres anteriors, i en el marc del principi de millora contínua del servei, l'Agència podrà requerir l'elaboració de nous lliurables i mètriques addicionals als ja definits, sempre que aquests resultin necessaris per garantir una execució eficient, homogènia i plenament alineada amb les necessitats operatives del Model i estiguin relacionats amb l'objecte del contracte.

6. Lot 3: Suport al seguiment dels plans de seguretat a l'àmbit sociosanitari (intermèdia) i salut mental

L'objecte del Lot 3 és donar suport al seguiment dels Plans de Seguretat de les entitats del Model de Ciberseguretat de l'àmbit sociosanitari (intermèdia) i la salut mental.

6.1. Funcions dels serveis objecte de la licitació pel Lot 3: Seguiment dels plans de seguretat a l'àmbit sociosanitari (intermèdia) i salut mental

6.1.1. Objectius del servei

L'objectiu principal d'aquest lot és donar suport a l'Agència en la interlocució i l'acompanyament de les entitats, mitjançant la recopilació sistemàtica de la informació de context necessària per facilitar-ne un assessorament adequat i garantir el correcte progrés de les seves actuacions en matèria de ciberseguretat. Així mateix, el servei assistirà l'Agència en la correcta execució de les activitats vinculades al Model de Ciberseguretat, d'acord amb les directrius establertes per la Direcció d'Estratègia d'Àmbits de Salut (DEA Salut).

El personal assignat actuarà com a punt de suport expert, participant en les activitats que involucrin les entitats amb l'objectiu d'aportar criteri tècnic, elevar les consultes que escaiguin als òrgans competents de l'Agència i garantir la traçabilitat de les qüestions plantejades. Igualment, qualsevol situació de risc detectada en relació amb una entitat serà degudament identificada i traslladada a l'Agència perquè aquesta pugui activar els mecanismes corresponents, tant en l'àmbit operatiu com en les àrees internes que escaiguin.

6.1.2. Funcions i activitats del servei

El servei inclou les tasques següents per al seguiment dels Plans de Seguretat amb les entitats d'atenció hospitalària i primària del SISCAT:

- **Donar suport a l'Agència en la interlocució amb les entitats**, contribuint al coneixement del seu context i a la vigilància del seu progrés en matèria de ciberseguretat mitjançant assessorament expert i d'acord amb les directrius establertes per l'Agència.
- **Assistir l'Agència en la revisió dels avenços, activitats, riscos, desviacions i necessitats** plantejades per les entitats, mitjançant la interlocució operativa que es determini en cada cas.
- **Donar suport al seguiment operatiu dels Plans de Seguretat** de les entitats assignades, en coherència amb els criteris i pautes definits per l'Agència.
- **Elaborar, recollir i consolidar els indicadors establerts pel Model**, aportant la informació requerida per a l'anàlisi i la presa de decisions per part de l'Agència.
- **Acompanyar l'Agència en reunions, activitats de revisió documental i suport a la implementació de mesures de seguretat**, actuant sempre com a assistència tècnica i no com a òrgan decisori.

- **Col·laborar amb la resta de serveis recurrents del Model**, d'acord amb les instruccions de l'Agència.
- **Donar suport en la gestió de dubtes de seguretat plantejats per les entitats**, incloent la seva tramitació, seguiment i tancament sota la supervisió de l'Agència.
- **Assistir en l'elaboració de documentació i plantilles** per al treball amb les entitats, d'acord amb els formats, criteris i procediments establerts per l'Agència.
- **Acompanyar les entitats en els seus processos de certificació i auditoria**, proporcionant assessorament i suport tècnic conforme a les indicacions de l'Agència.
- **Donar suport continu a les entitats** en presentacions, activitats i accions derivades de la interacció amb la resta de serveis del Model.
- **Proporcionar assistència en la interlocució amb altres serveis de l'Agència**, quan així es requereixi.
- **Generar informes d'estat de les entitats amb la periodicitat establerta** per l'Agència, ajustant-se a les instruccions de contingut, format i circuit de validació.
- **Utilitzar les eines de reporting i seguiment pròpies de l'Agència**, treballant de manera alineada amb les àrees internes per garantir la correcta planificació i facturació de les activitats del lot.

6.1.3. Volumetries previstes

D'acord amb l'abast funcional del servei i amb les necessitats de suport identificades per l'Agència, aquest lot prestarà assistència tècnica en el seguiment de 93 entitats de l'àmbit d'atenció intermèdia i de salut mental, integrades en el Model de Ciberseguretat del SISCAT.

Aquest volum és una estimació i com a tal podrà ser ajustat per l'Agència en funció de l'evolució del desplegament i de les necessitats operatives que es determinin durant la vigència del contracte.

6.1.4. Lliurables i mètriques del servei

S' haurà de preveure i garantir la generació, com a mínim, dels lliurables que s'indiquen a continuació.

Lliurable	Descripció	Freqüència
Context de l'entitat	Documentació que reculli tota la informació de context recopilada de cada entitat per al coneixement com a referent de la mateixa	Puntual a l'inici i quan es produeixin actualitzacions
Informe de Seguiment per Entitat	Estat del pla de seguretat, activitats, desviacions, riscos i necessitats.	Trimestral

Estat dels Plans de seguretat	Evolució en el temps dels plans de seguretat per cadascuna de les entitats.	Trimestral
Estat dels Perímetres	Evolució en el temps de les funcionalitats dels perímetres per entitat. Recull d'eines emprades per al perímetre.	Trimestral
Full d'activitats amb les entitats	Registre complet d'activitats executades i pendents per entitat a nivell de formació, simulacres, etc.	Mensual
Actes de reunions amb entitats	Acords, tasques i calendaris de les reunions amb cada entitat.	Després de cada reunió
Informe de desviacions i incidències	Resum dels incidents i desviacions detectades durant el seguiment.	Mensual
Informe de la situació actual d'una entitat	Resum de la situació actual per entitat.	Trimestral o semestral
Registre de Riscos Operatius d'Entitat	Identificació de situacions de risc amb les entitats i mesures correctores proposades	Mensual
Informe de situació anual	Mostra de la evolució anual agregada anual de l'entitat.	Anual

S'haurà de preveure i garantir la generació de, com a mínim, les mètriques que s'indiquen a continuació, amb la finalitat de donar suport a l'Agència en el seguiment, control i avaluació de la prestació del servei.

Mètriques	Descripció
Nombre d'entitats en seguiment	Estat agregat del conjunt d'entitats assignades i en seguiment: sociosanitària i salut mental.
Activitats amb les diferents entitats	Nombre de reunions de seguiment efectuades amb les entitats. Agregació per línies assistencials.
Activitats globals, segregades i individuals	Activitats executades dins del lot de forma global, per línies assistencials i per entitat. Indicació d'activitats dutes a terme i fites assolides.
Actualitzacions	Actualitzacions de la informació de context de les entitats: contactes, perímetre, etc.
Consultes	Consultes derivades i resoltes a través d'altres serveis del Model. Per exemple: - Consultes derivades cap a gestió de l'àmbit de Salut del SOC.

	- Consultes derivades cap a arquitectura.
Controls avaluats	Nombre de controls avaluats per cada entitat i de forma acumulada.
Lliurables generats	Nombre de lliurables generats i entregats.
Seguiments realitzats	Nombre de reunions de seguiment internes dels equips i de punts de control amb l'Agència.
Enquesta de Satisfacció	Puntuacions de les enquestes de satisfacció del model amb les entitats.
Informe Anual del Model de Ciberseguretat	Anàlisi global de resultats, maduresa assolida i propostes de millora.

Addicionalment al disposat als quadres anteriors, i en el marc del principi de millora contínua del servei, l'Agència podrà requerir l'elaboració de nous lliurables i mètriques addicionals als ja definits, sempre que aquests resultin necessaris per garantir una execució eficient, homogènia i plenament alineada amb les necessitats operatives del Model i estiguin relacionats amb l'objecte del contracte.

7. Condicions d'execució del servei

7.1. Horaris

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

A petició expressa de l'Agència, es podria demanar la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

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

7.2. Localització física.

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

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

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

7.3. 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.

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

L'adjudicatari de cada lot disposarà d'una figura que assumirà les tasques de **cap de servei / coordinador.** A aquest efecte, ha de 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.

N**o és necessari ofertar un perfil propi de cap de servei/coordinador**, sinó que aquestes funcions s'assignaran a un dels membres mínims requerits.

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 dona servei a l'Agència.

S'estima un total de 1760 hores per perfil de forma anual amb una dedicació total.

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de:

Lot 1: 8.800 hores anuals

Dins d'aquestes hores, s'estima el següent número d'hores anuals estimades pels perfils indicats:

Perfils del lot 1	Hores anuals estimades
Suport a la coordinació (perfil de consultor amb més de 5 anys d'experiència)	**8.800 hores**

Les hores indicades són una previsió estimada anual contemplada dins de la planificació del servei descrita en aquest plec.

Lot 2: 12.320 hores anuals

Dins d'aquestes hores, s'estima el següent número d'hores anuals estimades pels perfils indicats:

Perfils del lot 2	Hores anuals estimades
Suport al seguiment i cap de projecte del lot (perfil de consultor amb més de 5 anys d'experiència)	**1.760 hores**
Suport al seguiment (perfil de consultor amb 3 anys d'experiència en Ciberseguretat)	**10.560 hores**

Les hores indicades són una previsió estimada anual contemplada dins de la planificació del servei descrita en aquest plec.

Lots 3: 8.800 hores anuals

Dins d'aquestes hores, s'estima el següent número d'hores anuals estimades pels perfils indicats:

Perfils del lot 3	Hores anuals estimades
Suport al seguiment i cap de projecte del lot (perfil de consultor amb més de 5 anys d'experiència)	**1.760 hores**

Suport al seguiment (perfil de consultor amb més de 3 anys d'experiència en Ciberseguretat)	**7.040 hores**

Les hores indicades són una previsió estimada anual contemplada dins de la planificació del servei descrita en aquest plec.

Les hores totals estimades del contracte per cada un dels lots són les següents:

Lots	Hores totals estimades de la licitació per lots
Lot 1	**13.200 hores**
Lot 2	**18.480 hores**
Lot 3	**13.200 hores**

7.3.1. Perfils

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

PERFIL	REQUISITS	Lot
Suport a la coordinació (perfil de consultor amb 5 anys d' experiència en Ciberseguretat)	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 implicació en mínim tres projectes en els que hagi desenvolupat les següents funcions: • Lideratge de projectes i equips de treball multidisciplinars. • 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.	**1**

	• Suport administratiu en la planificació i formalització d'actes de reunions. Coneixements en: • Definició de projectes (metodologies, processos, eines, lliurables, etc.). • Coneixement avançat de models de gestió de seguretat de la informació (ISO, NIST i similars). • Coneixement de l'entorn normatiu i regulatori que aplica a la Ciberseguretat • Coneixement de l'entorn tecnològic (desenvolupament, gestió de serveis TIC, xarxes, gestió de proveïdors,...) • Coneixement de sistemes de seguretat tant tradicionals com emergents. • 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 etc.) 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). Habilitats/capacitats: • Capacitats de lideratge, gestió i direcció organitzativa • Capacitat de gestió d'equips i resolució de conflictes • Habilitats comunicatives avançades i capacitat de coordinació i interlocució amb altres equips. • Habilitats de comunicació, tant orals com escrites, en entorns i audiències diverses. • Capacitat analítica • Capacitat d'abstracció i síntesis per la recollida de resultats i generació d'indicadors concisos i de valor.	
Suport al seguiment i cap de projecte del lot (perfil de consultor amb 5 anys d' experiència en Ciberseguretat)	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 implicació en mínim tres projectes en els que hagi desenvolupat les següents funcions: • Lideratge de projectes i equips de treball multidisciplinars. • 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.	**2 i 3**

	• 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. • Suport administratiu en la planificació i formalització d'actes de reunions. Coneixements en: • Definició de projectes (metodologies, processos, eines, lliurables, etc.). • Coneixement avançat de models de gestió de seguretat de la informació (ISO, NIST i similars). • Coneixement de l'entorn normatiu i regulatori que aplica a la Ciberseguretat • Coneixement de l'entorn tecnològic (desenvolupament, gestió de serveis TIC, xarxes, gestió de proveïdors,...) • Coneixement de sistemes de seguretat tant tradicionals com emergents. • 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 etc.) 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). Habilitats/capacitats: • Capacitats de lideratge, gestió i direcció organitzativa • Capacitat de gestió d'equips i resolució de conflictes • Habilitats comunicatives avançades i capacitat de coordinació i interlocució amb altres equips. • Habilitats de comunicació, tant orals com escrites, en entorns i audiències diverses. • Capacitat analítica • Capacitat d'abstracció i síntesis per la recollida de resultats i generació d'indicadors concisos i de valor.	
Suport al seguiment (perfil de consultor amb 3 anys d' experiència en	Experiència professional 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 de tres projectes en els que hagi desenvolupat les següents funcions:	**2 i 3**

Ciberseguretat)	• Participació en projectes de seguretat amb equips de treball multidisciplinars. • Definició i/o seguiment de Plans Directors de Seguretat. • Anàlisi de riscos de seguretat i propostes de plans d'acció correctius. • 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: • Coneixement avançat de models de gestió de seguretat de la informació (ISO, NIST i similars). • Coneixement de l'entorn normatiu i regulatori que aplica a la Ciberseguretat • Coneixement de l'entorn tecnològic (desenvolupament, gestió de serveis TIC, xarxes, gestió de proveïdors,...) • Definició de projectes (metodologies, processos, eines, lliurables, etc.). • 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 etc.) 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). Habilitats: • Habilitats comunicatives i capacitat de treball i adaptació a equips multidisciplinari i a d' altres equips. • Capacitat d'adaptació • Habilitats de comunicació, tant orals com escrites, en entorns i audiències diverses. • Capacitat analítica • Actitud proactiva i resolutiva	

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

Aquests perfils mínims adscrits al contracte han estat establerts partint de la previsió dels volums màxims per l'execució adequada del servei, de forma estimativa. No estant obligada l'Agència de Ciberseguretat a adscriure efectivament tots els perfils, sinó únicament els que efectivament siguin

necessaris, sense que per aquest motiu l'adjudicatari tingui dret a percebre cap indemnització o compensació.

7.4. 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.

7.5. 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.

7.6. Eines i equipament per a la prestació de serveis.

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

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

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

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

L'Agència no proveirà:

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

En conseqüència, els adjudicataris hauran de:

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

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

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

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

7.7. 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.

[Indicar en cas que procedeixi la realització d'alguna actuació addicional]. NA

7.8. 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.
- 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.

7.9. 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.

7.10. **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

7.11. **Formació**

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

- Esquema nacional de seguretat especialment en els perfils de compliment específics relacionats amb l'àmbit de Salut.

- Formació en gestió de plans de seguretat o en aspectes tècnics relacionats amb les accions més habituals que apareixen representades en aquests plans per assessorar el millor possible a les entitats.

7.12. Contingència

L'adjudicatari haurà de proveir un pla de contingència, en cas de desastre de les instal·lacions principals, en unes instal·lacions alternatives (centre de gestió secundari) propietat de l'adjudicatari, que inclourà:

- 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.

7.13. 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.

7.14. Seguretat

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

7.14.1. 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.

7.14.2. 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.

7.14.3. 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.

7.14.4. 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.

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

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

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

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

7.14.6. 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.

7.14.7. 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.

7.14.8. 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.

7.14.9. Accés a la informació

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

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

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

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

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

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

7.16. 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.

7.17. Integració amb altres equips

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

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

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

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

- Creació d'un fons comú de coneixement sobre la seguretat de la informació.
- Creació de bucles de retroalimentació que facilitin una resposta àgil davant de qualsevol nova situació en matèria de seguretat.