Plec de prescripcions tècniques particulars que regeix la contractació basada relativa al suport especialitzat per l'adequació normativa a l'Esquema Nacional de Seguretat (ENS) en el sistema sanitari integral d'utilització pública de Catalunya (SISCAT).

Exp. CB25AMCONSL1011

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.

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, 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 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, incrementarà el nivell de protecció, resiliència i prevenció de més àmbits.

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 el Lot 1 - Consultoria de Ciberseguretat inclosa la vessant d'arquitectura. (AM.01.2024).

El present contracte podrà estar finançat fins a un 100% per la Unió Europea NextGenerationUE.

L'objecte de la licitació és donar suport especialitzat en l'adequació a l'ENS a un abast aproximat de 68 entitats del Sistema Sanitari Integral d'utilització pública de Catalunya (SISCAT) en un període d'entorn a 6 mesos. Algunes d'aquestes entitats es tracten de forma agrupada i per aquesta raó en alguns casos la interlocució realment es realitzarà amb menys entitats. S'estima que amb unes 60 entitats. En relació al compliment de l'ENS, a l'adequació s'hauran de contemplar els perfils de compliment específics següents: PCE-RFS i evolució al PCE-Salut.

Degut a aquest temps acotat, la metodologia i eines proposades per al suport han de ser àgils, eficients i innovadores. En definitiva, han de permetre aprofitar sinergies i que els resultats es puguin estendre i aplicar a totes les entitats. En aquest sentit, l'aproximació amb la que ha de treballar el servei és fonamentalment transversal.

Excepcionalment, s'ha de donar suport especialitzat en l'adequació a l'ENS de forma dedicada i personalitzada a certes entitats que tinguin sistemes de nova creació emmarcats principalment en el Plan de Atención Digital Personalizada (PADP). Aquest projecte forma part de l'Estratègia de Salut Digital 2021-2026 del Sistema Nacional de Salut i s'impulsa des del Servei Català de la Salut.

Amb l'objectiu de complir el punt anterior es considera necessari incloure dins d'aquest lot el **Suport Especialitzat en l'adequació a l'ENS** amb una aproximació transversal que oferirà assistència avançada i experta a l'Agència i a les entitats del SISCAT per:

- Elaborar plantilles de normatives que formaran part del marc normatiu transversal de ciberseguretat del SISCAT i que podran ser aplicables a totes les seves entitats.
- Elaborar les plantilles documentals necessàries per iniciar el procés d'adequació a l'ENS a partir dels documents que proporciona el CCN CERT. Principalment, els documents de valoració de serveis, categorització del sistema, declaració d'aplicabilitat i anàlisi de risc.
- Elaborar les plantilles documentals que cobreixin els aspectes de continuïtat de negoci requerits pel compliment dels perfils objectiu. Per exemple: BIA, RTO, RPO, PCN, etc.
- Facilitar les indicacions, models i exemples necessaris per fer possible que aquestes plantilles de normatives i documentals siguin fàcilment adaptables a les particularitats de les entitats.
- Crear material formatiu per comunicar les plantilles de normatives i documentals, i generar espais de treball i compartició de coneixement per treballar la particularització de les mateixes.
- Donar el suport que escaigui a les entitats de forma organitzada i propera per resoldre els dubtes que sorgeixin en l'adequació i evolució cap a la certificació. Crear una banc de coneixement per difondre a totes les entitats en cas que es consideri que és un tema transversal.
- Categoritzar com a mínim un sistema d'informació de cadascuna de les entitats dins l'àmbit d'aquesta licitació (segons la definició establerta pel CCN CERT per a la certificació en l'ENS) i elaborar el material necessari per donar els criteris i les pautes essencials per tal que les entitats ho puguin fer extensiu a la resta de sistemes d'informació de l'entitat de forma autònoma.
- Proposar solucions creatives i innovadores per impulsar i assessorar les entitats en l'adequació a l'ENS. Aquestes solucions han de permetre que el procés sigui ràpid i eficient per arribar en el mínim temps possible a l'objectiu de certificació.

- Elaborar un informe d'auditoria de compliment de les entitats per reflectir el grau de compliment del perfil específic de l'ENS seleccionat. Aquest document s'ha de realitzar en base a la informació disponible i les dades obtingudes durant el desenvolupament el servei.

És indispensable que aquest servei treballi de forma coordinada amb els serveis recurrents de l'Agència que formen part del model i que per tant ja tenen una via de comunicació i seguiment establerta amb les entitats. Aquests serveis són el Servei de suport de Governança i el servei de Conformitat amb l'ENS, el qual recull i avalua la conformitat de les evidències de compliment de l'ENS presentades per les entitats i les acompanya cap al procés final certificació en l'ENS.

La planificació i resultats obtinguts es compartiran amb els dos serveis esmentats anteriorment per alinear el correcte seguiment de les entitats. Les accions han d'estar coordinades per mantenir una alineació d'objectius clara amb les entitats. Aquests serveis també col·laboraran i facilitaran el primer contacte amb l'entitat.

Així mateix col·laboraran amb les resta de serveis més tècnics de l'Agència i les entitats si fos necessari quan, pels objectius del servei i les accions encomanades, es consideri necessari.

2.2 Lot 1: Serveis.

Antecedents

En els darrers anys, el sector sanitari s'ha consolidat com una de les infraestructures crítiques més exposades a ciberatacs a escala mundial. Diversos informes nacionals i internacionals han situat la sanitat pública entre els principals objectius de les amenaces digitals, amb un risc creixent derivat de la seva alta dependència tecnològica i de la sensibilitat de les dades que gestiona. Aquest increment del risc s'ha produït en paral·lel a una etapa de gran tensió assistencial, marcada per diferents escenaris que han posat a prova la capacitat de resposta del sistema.

D'una banda, la pandèmia de la COVID-19 va generar una situació excepcional, forçant una ràpida digitalització dels serveis i una ampliació significativa de l'ús de plataformes tecnològiques per a l'atenció remota i la gestió clínica. Aquesta acceleració va exposar encara més els sistemes d'informació sanitaris a riscos cibernètics, en un moment de màxima pressió i necessitat de continuïtat assistencial. D'altra banda, de forma estructural, el sistema de salut ha de fer front de manera cíclica a períodes de gran demanda, com les temporades de grip i altres virus respiratoris estacionals, que també incrementen la càrrega operativa i la dependència dels sistemes digitals.

Els sistemes d'informació sanitaris són absolutament crítics: suporten funcions essencials com el diagnòstic, el tractament, la gestió de recursos, la logística assistencial i la coordinació clínica. La seva disponibilitat, integritat i seguretat són fonamentals no només per garantir la qualitat de l'atenció, sinó per preservar la confiança ciutadana i assegurar el bon funcionament del conjunt de la societat.

En aquest context, el compliment normatiu en matèria de seguretat de la informació, i en particular l'adequació a l'Esquema Nacional de Seguretat (ENS), esdevé una prioritat estratègica. L'ENS proporciona un marc comú i auditable per garantir la protecció dels sistemes d'informació i les dades tractades per les entitats públiques, sent una peça clau per consolidar un model robust, sostenible i adaptat als requisits legals vigents.

Per fer-hi front amb garanties, és imprescindible estandarditzar la gestió de la seguretat, tant des del punt de vista tècnic com normatiu, aprofitant les economies d'escala derivades d'un enfocament coordinat i homogeni entre centres, i amb l'Agència. Aquest model permet optimitzar recursos, evitar duplicitats, i maximitzar l'impacte de les accions de seguretat arreu del sistema sanitari públic.

De cara als propers anys, es preveu una transformació profunda del model sanitari, marcat per l'expansió de la història clínica electrònica, la interoperabilitat entre sistemes, la medicina personalitzada, la intel·ligència artificial i la teleassistència. Aquesta evolució incrementarà la complexitat dels entorns tecnològics i, en conseqüència, la superfície d'exposició a ciberamenaces.

Això implicarà una exigència creixent per part de la ciutadania i dels organismes reguladors envers la seguretat, la traçabilitat i la disponibilitat de la informació sanitària. En aquest escenari, es preveu una intensificació de les exigències en el compliment normatiu dels sistemes d'informació sanitaris, tant per part dels òrgans reguladors com de la pròpia ciutadania, en línia amb els avenços tecnològics i l'expansió de serveis digitals en salut. Mes concretament, es requerirà que les entitats sanitàries:

- Integrin el compliment de l'ENS en la seva planificació estratègica i operativa, com a part estructural del seu funcionament habitual.
- Adoptin mecanismes de seguiment, control i millora contínua, que garanteixin no només l'obtenció sinó també el manteniment de la certificació ENS.
- Aconsegueixin maduresa en la gestió de la seguretat de la informació, tant en l'àmbit tècnic com organitzatiu, amb rols i processos clarament definits.
- Estiguin preparades per adaptar-se a l'evolució futura de l'ENS, així com a possibles nous marcs normatius de ciberseguretat en l'àmbit públic i sanitari.

En aquest sentit, el servei que es proposa en aquesta licitació no només respon a la necessitat d'adequació actual al marc ENS, sinó que s'alinea amb una visió a mig i llarg termini, orientada a consolidar una cultura de compliment, resiliència i protecció proactiva dels serveis essencials de salut. El servei actuarà com a palanca de transformació cap a una gestió més madura, eficient i coordinada del compliment normatiu, assegurant que els centres sanitaris públics estiguin preparats per fer front als desafiaments presents i futurs en matèria de seguretat de la informació, mitjançant un acompanyament expert i estructurat que contribueixi a enfortir la seguretat dels serveis essencials de salut i protegir un pilar fonamental del benestar col·lectiu.

2.2.1 Objecte i abast del servei de suport especialitzat en l'adequació a l'ENS.

El servei de **Suport Especialitzat en l'adequació a l'ENS** està dirigit tant a l'Agència, com directament a les entitats. Tot i dirigir-se a les entitats les tasques s'efectuaran de forma planificada i coordinada amb els serveis existents recurrents del model de ciberseguretat desplegat per l'Agència en aquestes entitats. Concretament, amb l'equip del servei de suport de governança i el servei de conformitat amb l'ENS.

Totes les accions han de ser planificades per ser executades i finalitzades fins dels terminis als que es troba subjecte per tractar-se de fons europeus. La data màxima de finalització no pot ser en cap cas posterior al 30 de juny del 2026.

El servei està dirigit a un objectiu clar, l'impuls en l'adequació a l'ENS per les 68 entitats proveïdores del SISCAT d'atenció especialitzada o hospitalària, que actualment tenen el model de ciberseguretat desplegat. Els perfils específics de compliment de l'ENS que es contemplen són els següents: PCE-RFS i PCE-Salut.

Dins d'aquest impuls es preveuen les següents tasques o accions:

- Disposar d'un **marc normatiu transversal de ciberseguretat per al SISCAT**. Dins d'aquest objectiu es contempla completar i posar a disposició de les entitats un marc normatiu transversal de ciberseguretat del SISCAT alineat amb els requeriments de l'Esquema Nacional de Seguretat (ENS) i, en especial, els perfils específics de compliment seleccionats.

El disseny de l'estructura del marc normatiu transversal de ciberseguretat del SISCAT estableix que en un alt percentatge es podran fer servir d'una forma directa el cos normatiu de ciberseguretat ja definit per a la Generalitat de Catalunya. Es calcula de forma aproximada que en un 70% dels casos les normatives necessàries es cobriran amb les ja existents al cos normatiu de la Generalitat de Catalunya. El 30% restant serà necessari desenvolupar-lo tenint en compte les particularitats de les entitats SISCAT en un primer terme i fent-les perquè siguin adaptables a les especificitats de les entitats a les que els és d'aplicació.

En aquest sentit, totes les normatives que actualment formin part del cos normatiu de ciberseguretat de la Generalitat de Catalunya hauran de ser revisades per confirmar la seva aplicació directa al SISCAT i per valorar si existeixen particularitats que calgui definir o deixar per omplir en el cas de les entitats del SISCAT. Així mateix, s'hauran d'identificar les normatives noves que no estiguin presents i que siguin necessàries per completar el marc normatiu de ciberseguretat del SISCAT i complir amb l'ENS.

Com a conclusió de l'anàlisi anterior, s'hauran d'elaborar les plantilles de les normatives que no siguin aplicables de forma directa i que requereixin d'una adaptació d'acord amb les particularitats de les entitats del SISCAT. També s'hauran d'elaborar les plantilles de les normatives noves que no estiguin presents.

- Elaborar les plantilles documentals necessàries per iniciar el procés d'adequació a l'ENS a partir dels documents que proporcionar el CCN CERT. Principalment, els documents de valoració de serveis, categorització del sistema, declaració d'aplicabilitat i anàlisi de risc.
- Elaborar les plantilles documentals que cobreixin els aspectes de continuïtat de negoci requerits pel compliment dels perfils objectiu. Per exemple: BIA, RTO, RPO, PCN, etc.
- Facilitar les indicacions, models i exemples necessaris per fer possible que aquestes plantilles de normatives i documentals siguin fàcilment adaptables a les particularitats de les entitats.
- Crear material formatiu per comunicar les plantilles de normatives i documentals elaborades en l'àmbit d'aquesta licitació a les entitats implicades, i generar espais de treball i compartició de coneixement per treballar la particularització de les mateixes. Es podran contemplar, entre d'altres la realització de formacions grupals.
- Acompanyar i donar el suport que escaigui a les entitats de forma organitzada i propera per resoldre els dubtes que sorgeixin en l'adequació i evolució cap a la certificació. Generar espais compartits amb les entitats per tractar les temàtiques que es necessiti tractar de forma més transversal. Per exemple: cursos de formació agrupant per tipologia d'entitats o per temàtiques a abordar, per dominis de l'ENS, per normatives concretes, FAQs, espais de dubtes, bancs de coneixement, etc.
- Realitzar formacions grupals amb les entitats implicades. Aquestes sessions ha de conscienciar i facilitar la comprensió compartida de les obligacions, promoure la correcta aplicació dels procediments i assegurar que els responsables i participants disposin dels coneixements necessaris per actualitzar i conservar la documentació i els registres de manera continuada.
- Accions de **suport individual amb les entitats proveïdores del SISCAT:**
  - Categoritzar com a mínim un sistema d'informació de cadascuna de les entitats dins l'àmbit d'aquesta licitació (segons la definició establerta pel CCN CERT per a la certificació en l'ENS) i elaborar el material necessari per donar els criteris i les pautes necessàries per tal que les entitats ho pugin fer extensiu a la resta de sistemes d'informació de l'entitat de forma autònoma. No obstant, caldrà mantenir el suport necessari per fer correctament aquesta categorització i fer sessions de formació individuals o grupals amb les entitats per al correcte traspàs de coneixement.
  - Revisar quines polítiques i normatives pròpies estan disponibles a les entitats per tenir una foto clara de l'estat actual de les mateixes. Aquest suport documental és especialment rellevant en la fase de preparació per a l'auditoria de certificació o recertificació, ja que permet disposar de tota la base normativa pròpia validada i adaptada, amb la qual justificar

el compliment davant els òrgans certificadors. Així mateix, contribueix de forma decisiva a la maduresa del sistema de gestió de seguretat de la informació (SGSI) i a la consolidació d'una cultura de seguretat sòlida i sostenible.

- Treballar amb l'entitat i amb els serveis de suport de governança i conformitat ENS per definir una planificació factible per fixar una data objectiu de certificació i posterior evolució.
- Elaborar un informe d'auditoria de compliment de les entitats per reflectir el grau de compliment del perfil específic de l'ENS seleccionat. Aquest document s'ha de realitzar en base a la informació disponible i les dades obtingudes durant el desenvolupament el servei.

Excepcionalment, s'ha de donar suport especialitzat en l'adequació a l'ENS de forma dedicada i personalitzada a certes entitats que tinguin sistemes de nova creació emmarcats principalment en el Plan de Atención Digital Personalizada (PADP). Aquest projecte forma part de l'Estratègia de Salut Digital 2021-2026 del Sistema Nacional de Salut i s'impulsa des del Servei Català de la Salut.

- **Accions de coordinació amb el serveis i equips de l'Agència**. Els principals serveis relacionats amb l'àmbit de la licitació són:

  - Servei de suport de governança per compartir la planificació, els resultats obtinguts i la foto de l'estat d'adequació actual i alinear el correcte seguiment de les entitats. Així mateix, actualitzar adequadament les accions dels Plans de seguretat que s'estan seguint amb les entitats.
  - Servei de conformitat amb l'ENS per compartir l'estat d'adequació i poder avançar cap a la correcte recollida d'evidències que anirà avaluant aquest servei de conformitat per avançar cap a l'objectiu de certificació.

  Les accions han d'estar coordinades entre els diferents serveis per mantenir una alineació d'objectius clara amb les entitats. Aquests serveis també col·laboraran i facilitaran els primers contactes amb l'entitat.

  Així mateix, el servei objecte d'aquesta licitació ha de col·laborar amb les resta de serveis més tècnics de l'Agència i les entitats si fos necessari pels objectius del servei i les accions encomanades es consideri necessari.

  Per dinamitzar la col·laboració, s'hauran de realitzar de formacions grupals amb l'equip de suport de governança i de conformitat amb l'ENS, amb l'objectiu de compartir el coneixement i treballar-lo de forma més ràpida i efectiva amb les entitats.

Els documents es lliuraran en formats editables i adaptats a la realitat organitzativa i tècnica de cada entitat. El proveïdor haurà de treballar col·laborativament amb el personal intern, garantint una correcta transferència de coneixement i fomentant l'autonomia de l'organització en la gestió posterior dels seus documents.

Aquest suport, juntament amb les activitats formatives, contribuirà de manera decisiva a la maduresa normativa del sistema de seguretat de la informació, i facilitarà tant l'èxit en les auditories com el manteniment d'un sistema viu, revisable i sostenible.

És necessari idear i proposar solucions creatives i innovadores que permetin impulsar i assessorar aquesta adequació ràpida i eficient amb les entitats per arribar en el mínim temps possible a l'objectiu de certificació, i sempre respectant els terminis que determina el fons per la seva execució, i que en cap cas pot superar el 30 de juny del 2026.

Abast

S'inclouen a l'abast les tasques descrites anteriorment amb totes les entitats del SISCAT integrades en el model de ciberseguretat desplegat per l'Agència. Es tracta de 68 entitats. Algunes d'elles es tracten de forma agrupada i per aquesta raó en alguns casos la interlocució realment es realitza amb 60 entitats.

Exclusió de l'abast

Queda fora l'abast la redacció individualitzada de les polítiques i normatives de l'entitat. El servei sí redacta documents transversals en format plantilla per aquells punts que calgui particularitzar i donarà el suport necessari a l'entitat perquè aquesta les particularitzi tenint en compte les seves particularitats.

Queden expressament exclosos d'aquest servei els treballs relacionats amb **canvis en aplicacions, desenvolupaments de programari, instal·lacions d'aplicacions o modificacions tècniques en els sistemes d'informació**. Aquest tipus d'activitats queden fora de l'objecte del suport documental i hauran de ser gestionades per altres serveis o equips especialitzats.

2.2.2 Característiques del servei de suport especialitzat en l'adequació a l'ENS.

El **Suport Especialitzat en l'adequació a l'ENS** serà un servei orientat a proporcionar assistència avançada i continuada a les entitats del SISCAT des d'una perspectiva transversal. No es preveu una adequació dedicada de forma exclusiva amb totes i cadascuna de les entitats però si un suport individualitzat amb les mateixes i que s'adapti al seu ritme amb l'objectiu de facilitar al màxim la seva adequació a l'ENS.

El servei establirà una metodologia estructurada que permetrà abordar totes les accions encomanades que s'han descrit anteriorment.

Es treballarà en estreta col·laboració amb els equips interns de cada entitat identificats com a interlocutors segons les accions a escometre, assegurant que els lliurables resultants del servei siguin aplicables a la seva realitat operativa i estiguin alineats amb el nivell ENS corresponent. Si dins del projecte s'assoleix l'objectiu més baix es treballarà per avançar en el següent nivell. Per exemple: si una entitat obtingués durant l'execució del contracte la certificació en PCE-RFS es continuarà durant la durada del servei en l'evolució cap el PCE-Salud.

Així mateix, pel correcte desenvolupament del servei, s'haurà de tenir en compte el context de les entitats i tota la documentació i material que aquestes tinguin disponibles i que pugui estar en relació amb el compliment de l'ENS.

El servei impulsarà la creació d'una **base de coneixement** pròpia, que recollirà l'experiència adquirida, les lliçons apreses i les bones pràctiques detectades durant l'operativa. Aquesta base permetrà elaborar noves peces documentals i plantilles de manera més àgil, eficient i coherent, aportant valor amb l'objectiu d'accelerar l'adequació de totes les entitats del SISCAT.

Totes les actuacions es realitzaran amb un enfocament clarament orientat a la protecció de la informació, la continuïtat assistencial i la resiliència digital. El servei haurà de complir els terminis i els criteris de qualitat establerts, mantenint una gestió, coordinació constant i comunicació fluida amb l'Agència i amb les entitats.

En la fase inicial del servei es realitzarà una reunió d'inici, individual o grupal, amb tots els actors clau de l'Agència i de les entitats per explicar l'objectiu i metodologia a seguir. L'ordre del dia de la reunió d'inici contindrà com a mínim els següents punts:

- Presentació dels objectius, l'abast i les exclusions del servei.
- Definició dels rols i responsabilitats.
- Equip de treball del servei.
- Lliurables del servei.
- Pla de treball detallat amb terminis i responsables.

Així mateix, durant la fase final del servei, el servei realitzarà una reunió de tancament amb l'objectiu d'explicar les principals fites aconseguides, els indicadors i resultats del projecte. De forma complementària, prepararà un informe de l'estat final d'adequació al nivell ENS corresponent a cada entitat i a nivell global de servei.

Tota la documentació generada durant el desenvolupament del servei s'emmagatzemarà al repositori corporatiu. Es Mantindrà un registre mestre amb l'estat i la traçabilitat de cada peça.

Entre d'altres, s'hauran d'elaborar els següents lliurables:

1. **Inventari inicial del marc normatiu transversal de ciberseguretat per al SISCAT i plantilles documentals**
    - Relació de documents a elaborar o actualitzar, agrupats per àmbit i tipologia.
    - Inclou estat inicial, prioritat, planificació i assignació de responsabilitats.
2. **Esborranys inicials dels documents validada prèviament amb alguna de les entitats que es prengui com a mostra**
    - Primera versió de cada document
    - Pot incloure notes o comentaris contextuals per orientar la validació.
3. **Registre d'iteracions i observacions per document**
    - Fitxa amb l'historial de versions, aportacions i acords.
    - Garantia de traçabilitat i qualitat dels continguts.
4. **Versió final dels documents**
    - Inclou data de validació, número de versió i format definitiu.
5. **Informe d'adequació al nivell ENS corresponent per entitat**
    - Document justificatiu que acredita que cada peça elaborada s'ajusta al nivell ENS objectiu.
    - Suport complementari per a processos d'auditoria.
6. **Criteris d'integració i arxiu documental**

- Instruccions per a la classificació, codificació i permisos dins del repositori corporatiu (p. ex. SharePoint).
- Inclou estructura de carpetes i comprovació de consistència.

7. **Material i actes de les formacions grupals a les entitats i/o Agència**
   - Presentacions, guies o manuals utilitzats a les sessions formatives.
   - Actes resum amb participants, temes tractats i conclusions sobre el manteniment del cos d'evidències.
8. Elaborar un informe d'auditoria de compliment de les entitats per reflectir el grau de compliment del perfil específic de l'ENS seleccionat. Aquest document s'ha de realitzar en base a la informació disponible i les dades obtingudes durant el desenvolupament el servei.
9. **Informe final global d'adequació a l'ENS**
   - Informe final d'estat global en relació a l'adequació a l'ENS de totes les entitats assolida a la finalització del servei.
   - Informe final global de les plantilles generades i la seva utilització per part de les entitats

Excepcionalment, s'ha de donar suport especialitzat en l'adequació a l'ENS de forma dedicada i personalitzada a certes entitats que tinguin sistemes de nova creació emmarcats principalment en el Plan de Atención Digital Personalizada (PADP). Aquest projecte forma part de l'Estratègia de Salut Digital 2021-2026 del Sistema Nacional de Salut i s'impulsa des del Servei Català de la Salut.

Durant la durada del servei, s'assegurarà la qualitat i l'eficiència de totes les fases. Es mantindran canals de comunicació constants amb les entitats i l'Agència, es supervisarà indicadors de progrés, s'identificaran els riscos i s'aplicaran mesures correctores quan calgui. En aquest sentit, el licitador,

- Proposarà els indicadors que permetin fer el seguiment del servei, mesurar el grau d'execució, la qualitat dels lliuraments, la seva validació formal amb les entitats i amb l'Agència, i l'efectivitat de les formacions, entre d'altres. Aquesta proposta haurà de ser consensuada amb l'Agència i les entitats.
- Organitzarà reunions periòdiques per fer el seguiment.
- Supervisarà indicadors clau i detectarà bloquejos. Així mateix, aplicarà mesures correctores quan sigui necessari.
- Proporcionarà un quadre de comandament que inclogui:
  - **Indicadors clau (KPIs)** sobre el grau d'avanços en la confecció del suport documental, l'estat, els terminis, les iteracions i la qualitat dels lliuraments.
  - Capacitat d'**alerta i detecció de desviacions**, per facilitar una gestió proactiva de l'operativa.
  - **Integració amb el model de dades corporatiu**, assegurant la seva coherència i disponibilitat per a la presa de decisions.

Aquest quadre actuarà com a **eina clau de governança**, oferint una visió transversal i objectiva del desplegament del servei i facilitant el seu alineament amb les polítiques institucionals de seguretat de la informació.

3 Condicions d'execució del servei

3.1 Horaris

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

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

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

3.2 Localització física.

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

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

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

3.3 Equip de treball

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

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

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.
- Habilitat per identificar, analitzar i resoldre problemes.
- Capacitat de treball sota pressió.
- Coneixement de català, castellà i d'anglès, parlat i escrit.

- Ampli coneixement legal, tecnològic i de negoci de seguretat informàtica i de l'entorn de l'administració pública.
- Altres necessaris per al bon desenvolupament dels serveis.

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** o assignarà les seves funcions a una de les figures del projecte sens prejudici de les funcions assignades a aquesta. A aquest efecte, ha de assumir les següents responsabilitats.

Funcions i tasques del Cap de Servei

Aquest perfil, en base al model de relació de l'Agència, es coordinarà amb els responsables del servei per part de l'Agència **com a punt de contacte principal**, per tal de garantir la correcta execució de les capes de gestió, administració i servei. A aquest efecte, ha de responsabilitzar-se de que els següents punts s'executen per part del servei de manera correcta i continua:

- Garantir que l'Agència rebi els informes de gestió acordats i realitzar el seguiment econòmic i d'activitat amb els interlocutors de l'Agència.
- Garantir la transparència en el control de gestió per tal d'agilitzar el procés de seguiment i facturació.
- Coordinació amb la resta d'àrees i equips de l'Agència assegurant una bona col·laboració entre els diferents agents implicats.
- Generació, implementació i càlcul de les mètriques i els indicadors del servei.
- Generació d'informes referents a incidències de servei, actes, informes executius, informes de resultats o informes de situació, entre d'altres, assegurant sempre la qualitat tècnica i executiva dels informes.
- Suport a la resolució de conflictes i incidències.
- Consolidar i aportar a l'Agència les informacions objectives i subjectives que permetin a la Direcció la presa de decisions operatives, tàctiques i estratègiques relacionades amb el contracte.
- Assegurament de la qualitat del servei prestat i dels lliurables generats (Quality Assurance).
- Gestió de riscos operatius del servei.
- Identificació d'oportunitats de millora.

Funcions i tasques del Cap de Projecte

El **Cap de Projecte** assumirà la responsabilitat de **planificar, coordinar, supervisar i avaluar** totes les activitats necessàries per a l'operativa del servei. Serà la figura clau per garantir que els objectius es compleixin dins els terminis establerts, amb els nivells de qualitat requerits i amb una gestió eficient dels recursos humans i tecnològics.

Les seves principals tasques seran:

Planificació estratègica i definició de l'abast

- Establirà, conjuntament amb les entitats els objectius específics i les prioritats de cada projecte d'adequació.
- Definirà el calendari global i els terminis per a cada fase: inventari, redacció, validació, formació i suport a l'auditoria.
- Determinarà els recursos necessaris (redactors, revisors, tècnics de suport, etc.) i assignarà responsabilitats.

Coordinació de l'equip i gestió de recursos

- Dirigirà i supervisarà l'equip del servei, vetllant per l'assignació equilibrada de tasques i la correcta execució de cada activitat.
- Convocarà reunions de seguiment internes per revisar l'estat dels treballs, anticipar riscos i resoldre incidències.
- Fomentarà la col·laboració entre els diferents perfils (redactors, formadors, tècnics) per assegurar la coherència del conjunt documental.

Relació amb les entitats beneficiàries

- Mantindrà una comunicació fluida amb els responsables de seguretat de la informació i amb els equips dels serveis de suport a la Governança i de conformitat amb l'ENS, els quals actuen com a interlocutors amb les entitats.
- Presentarà l'abast dels treballs, els terminis i els lliuraments previstos, recollint expectatives i requeriments.
- Coordinarà la recollida de comentaris i observacions de les entitats, assegurant que quedin registrats i traçats.

Supervisió de la generació documental

- Validarà l'inventari inicial i les prioritats de treball.
- Revisarà els esborranys clau abans d'enviar-los a validació formal.
- Comprovarà que els documents mantinguin l'alineament amb els controls ENS i amb el nivell aplicable (bàsic, mitjà o alt).
- Vetllarà per l'ús correcte de plantilles i per l'actualització constant de la base de coneixement.

Control de qualitat i traçabilitat

- Establirà criteris de qualitat per a cada tipologia documental i en verificarà el compliment.
- Assegurarà que tots els documents tinguin metadades completes, versió correcta i estat actualitzat a l'eina de govern.
- Validarà que els lliuraments i acords amb les entitats quedin registrats i vinculats als controls ENS pertinents.

Impuls de l'eina tecnològica i de la base de coneixement

- Liderarà el disseny i desplegament de l'eina que governarà l'operativa del servei.
- Definirà, juntament amb l'equip tècnic, els requeriments funcionals: repositori, control de versions, gestió d'entitats, comentaris, mapeig amb controls ENS, etc.
- Vetllarà per l'actualització permanent de la base de coneixement i per l'ús eficient de plantilles i models.

Formació i sensibilització

- Planificarà i aprovarà els continguts de les formacions grupals destinades a equips interns, serveis que ho necessitin i externs de les entitats.
- Assegurarà que aquestes sessions reforcin la capacitat de mantenir i actualitzar el cos documental i les evidències.
- Validarà que les conclusions i actes de les sessions quedin arxivades i disponibles.

Suport a auditories i recertificacions

- Donarà suport a la preparació dels dossiers d'auditoria i les respostes a observacions o no conformitats.
- Supervisarà els terminis de resolució i la generació de noves versions dels documents afectats.
- Farà d'enllaç entre l'equip redactor i els auditors, assegurant una comunicació clara i eficaç.

Seguiment d'indicadors i informes de progrés

- Monitorarà els KPIs definits (documents planificats vs. lliurats, qualitat, iteracions, cobertura de controls ENS, temps de resposta, etc.).
- Presentarà informes periòdics a la direcció o als òrgans de govern del servei, destacant l'estat, riscos i oportunitats de millora.
- Proposarà accions correctores quan s'identifiquin desviacions.

Millora contínua i sostenibilitat

- Promourà revisions periòdiques de processos i plantilles per mantenir la coherència i agilitat del servei.
- Impulsarà l'adopció de lliçons apreses i bones pràctiques dins la base de coneixement.
- Vetllarà perquè el servei evolucioni amb els canvis normatius o amb les necessitats de les entitats.

Resultat esperat

El **Cap de Projecte** garantirà que el **Suport Especialitzat en l'adequació a l'ENS** s'executi amb eficàcia, transparència i qualitat. Haurà assegurat que:

- Els objectius i terminis s'han complert.
- Els documents i evidències estan correctament elaborats, validats i arxivats.
- L'eina tecnològica funciona com a punt únic de govern i traçabilitat.
- Les entitats han rebut suport personalitzat i tenen capacitat per mantenir la seva documentació.
- El servei disposa d'una base de coneixement viva que millora l'agilitat i el valor dels resultats.

El **Cap de Projecte** assumirà tant les funcions descrites en aquest apartat com les tasques inherents a l'objecte de la licitació.

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 **[10.290] hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	Hores anuals mínimes estimades
1 Cap de projecte (Consultor expert de seguretat amb més de 5 anys d'experiència amb coneixement específic de l'ENS)	**1.715**
5 Consultor expert de seguretat amb més de 5 anys d'experiència amb coneixement específic de l'ENS	**8.575**

Els requisits anteriors s'han d'entendre com a mínims aproximats, podent-se ampliar en la proposta tècnica. El cap de servei participarà de forma dedicada al servei afegint a les seves tasques les de coordinació i reporting corresponent a les funcions de cap de servei.

3.3.1 Perfils

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

PERFIL	REQUISITS
Cap de projecte (Consultor expert de seguretat amb més de 5 anys d'experiència amb coneixement específic de l'ENS)	**Formació acadèmica** • Grau o enginyeria en Informàtica, Telecomunicacions o Ciències de la Computació. **Certificacions professionals (altament valorades)** • **Seguretat i compliment normatiu:** ○ ISO/IEC 27001 (Lead Implementer o Lead Auditor). **Experiència professional (mínim 5 anys)** • Gestió de projectes de seguretat i adequació normativa. • Participació en projectes d'auditoria (en base a metodologia CCN-CERT, ISO27001 o metodologies similars) i anàlisi de riscos (en base a metodologia CCN-CERT, ISO27005 o metodologies similars). • Experiència en la construcció de marcs normatius o elaboració de normes o estàndards de compliment normatiu

	• Experiència amb plans de continuïtat de negoci i resposta davant incidències (alineats amb ISO 22301 i ENS). • Experiència en plataformes corporatives Microsoft 365 (SharePoint, PowerAutomate i PowerBI), aplicades a entorns de gestió documental i fluxos de treball. • Elaboració i seguiment de KPIs i quadres de comandament en temps real. • Participació en projectes amb administracions públiques o entorns regulats. **Competències clau** • Ampli coneixement normatiu en l'ENS, perfils de compliment específics de l'ENS, ISO 27001, ISO 22301, RGPD, LOPDGDD, estàndards CCN-CERT i altres normatives de ciberseguretat vigents aplicables a l'àmbit de Salut. • Lideratge d'equips i capacitat de gestió de stakeholders en entorns públics i regulats. • Habilitats de comunicació a tots els nivells, operatius i directius. Comunicació clara i efectiva amb els interlocutors, interns, externs i de diferents perfils, operatius i de direcció. • Gestió del canvi i comunicació, amb habilitat per dirigir sessions kick-off, formació i coordinació d'entitats diverses. • Pensament analític i orientació a resultats. • Capacitat de planificació i organització: control de terminis, cronogrames i assegurament de lliurables.
Consultor expert de seguretat amb més de 5 anys d'experiència amb coneixement específic de l'ENS	**Formació acadèmica** • Grau en Enginyeria Informàtica, Telecomunicacions, Ciències de la Computació o similar. **Certificacions professionals** • **Seguretat i compliment normatiu:** ○ ISO/IEC 27001 (Implementer o Auditor). **Experiència professional (mínim 5 anys)** • Gestió de projectes de seguretat i adequació normativa. • Participació en projectes d'auditoria (en base a metodologia CCN-CERT, ISO27001 o metodologies similars) i anàlisi de riscos (en base a metodologia CCN-CERT, ISO27005 o metodologies similars). • Experiència en la construcció de marcs normatius o elaboració de normes o estàndards de compliment normatiu

	• Experiència amb plans de continuïtat de negoci i resposta davant incidències (alineats amb ISO 22301 i ENS). • Experiència en anàlisi i categorització de sistemes d'informació, elaboració de documents d'anàlisi de riscos i declaració d'aplicabilitat. • Pràctica en auditories de compliment normatiu. • Ús habitual de SharePoint per a la gestió documental. Almenys 1 dels perfils hauria de disposar de coneixements de configuració i automatització en la plataforma Microsoft 365 (SharePoint, PowerAutomate i PowerBI). • Coneixements aplicats de PowerBI per al seguiment de KPIs i indicadors de projecte. **Competències clau** • Habilitats en la redacció de documents de caràcter normatiu i informes • Coneixement pràctic i actualitzat del marc normatiu ENS i la seva aplicació real. • Capacitat analítica per identificar deficiències i proposar accions correctores concretes. • Comunicació clara i efectiva amb els interlocutors, interns, externs i de diferents perfils, operatius i de direcció. • Organització i traçabilitat, capaç de documentar i registrar adequadament cada pas del procés. • Treball en equip i capacitat de coordinar-se sota la direcció del Cap de Servei, mantenint alineació amb els objectius generals del projecte.

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

3.4 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte basat el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies laborables a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència a l'empresa adjudicatària del contracte basat. L'adjudicatari haurà de presentar en un termini màxim de 10 dies laborables a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució. Si l'objecte del contracte basat ho requereix, aquest aspecte es podrà concretar en aquest.

3.5 Control de rotació

L'estabilitat dels recursos del servei amb coneixement i compromís és molt important per a la correcta prestació del servei.

L'empresa adjudicatària del contracte basat podrà fer canvis en l'equip de treball durant l'execució del contracte, però ho haurà de notificar per escrit a l'Agència amb una antelació mínima de 14 dies naturals, justificant el canvi i informant del perfil i característiques de la persona que s'incorpora. L'Agència comprovarà que la persona a incorporar compleix amb les condicions curriculars del component de l'equip que substitueixi.

L'empresa assumirà la selecció de les persones de nova incorporació, la coexistència en el servei del personal sortint i l'entrant sense cost per l'Agència, assegurant el correcte traspàs de coneixement en els següents 15 dies i duent a terme els controls necessaris per garantir-lo entenent, per tant, la no facturació d'aquests dies d'adaptació i traspàs. Sens perjudici que si s'escau es puguin aplicar els ANS corresponents per rotació excessiva.

En cap cas la substitució de personal suposarà un cost addicional, havent-se de garantir que el servei no es vegi afectat per aquest canvi. Si l'objecte del contracte basat ho requereix, aquest aspecte es podrà concretar en el contracte basat.

3.6 Eines i equipament per a la prestació de serveis.

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

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

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

L'Agència no proveirà:

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

En conseqüència, els adjudicataris hauran de:

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

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

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

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

3.7 Gestió del coneixement

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

Igualment, i tal com es defineix en aquest mateix plec, haurà de dur a terme sessions de formació a les àrees de l'Agència que ho requereixin durant l'execució del contracte i a la seva finalització per assegurar el correcte traspàs de coneixement.

3.8 Seguretat Corporativa

Un cop adjudicat el contracte basat, tant l'empresa adjudicatària com el personal de l'empresa adjudicatària s'haurà de sotmetre a les polítiques i regulacions internes que estableix l'àrea de Seguretat Corporativa en matèria de seguretat de la informació, com a mínim i no limitant-se a:

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- Facilitar l'accés en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de l'Agència (sigui o no per l'exercici de la seva funció).

- Acceptar les normes i polítiques que estableix l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.
- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'àrea de Mitjans Tècnics per fer el desplegament de polítiques i controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.
- Els equips, així com la informació resident dels mateixos serà sempre custodiada per l'Agència.
- Garantir l'estabilitat dels equips (reduint al mínim la rotació de personal).
- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (ENS, LOPDGDD, GDPR, LSSI).

A la finalització del contracte, l'adjudicatari del contracte basat quedarà obligat al lliurament o destrucció en cas de ser sol·licitada, de qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

3.9 Control de Gestió

L'empresa adjudicatària del contracte basat, i en especial el cap de servei, haurà de col·laborar amb el responsable de la planificació pressupostària i el control de gestió de l'Agència per tal:

- De complir amb el model de seguiment econòmic i planificació en termes de capacitat i execució de tasques.
- D'ajustar-se als procediments de facturació que determini l'Agència.
- De conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència, d'acord amb els procediments establerts.
- D'exercir la gestió del contracte amb capacitats de *forecast.*
- Realitzar el *reporting* en les eines proporcionades per l'Agència amb els següents conceptes.
- Fitxer mestre de persones.
- Fitxer mestre de projectes i activitats.
- Estimació de recursos per projecte.
- Seguiment dels riscos.
- Seguiment del consum de recursos.
- Imputació de temps i activitats.
- Assignació de tasques a persones.
- Memòria d'activitat del contracte.
- Facturació i Conformació de factures.

L'adjudicatari proporcionarà la seva total col·laboració per a la realització d'auditories i la verificació del compliment dels compromisos. Aquestes auditories, realitzades en qualsevol de les instal·lacions involucrades en la prestació del servei, podran ser portades a terme per personal de l'Agència o sol·licitades a tercers. No serà necessari fer una notificació prèvia per a la realització de tasques d'auditoria que no requereixin la col·laboració activa per part del personal de l'adjudicatari. En el cas

en què sigui necessària aquesta col·laboració, l'Agència farà una notificació amb dues setmanes d'antelació.

3.10 Documentació.

L'Agència és el propietari de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris i el seu personal i subcontractats que destini a l'execució dels serveis. L'adjudicatari s'encarregarà de disposar de totes les autoritzacions i permisos necessaris per tal de poder donar compliment a aquesta previsió, essent responsabilitat de l'adjudicatari qualsevol pagament o reclamació relativa a aquesta manca d'autoritzacions.

Els responsable de servei de l'Agència serà els responsable de la validació i aprovació dels documents elaborats pel personal de l'adjudicatari. En cas que la qualitat dels documents sigui molt baixa o de manera recurrent i/o perllongada en el temps de prestació dels serveis no assoleixi els nivells requerits s'aplicaran les penalitzacions establertes en la present licitació.

L'adjudicatari haurà de mantenir la documentació actualitzada en el sistema de gestió documental que l'Agència proporcioni per tal efecte

3.11 Formació

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

3.12 Contingència

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 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.
    - Personal de l'Agència, o de terceres parts determinades per aquest, per a la correcta gestió del servei.
- Pla i execució de proves per validar la solució de contingència implementada, amb la periodicitat que l'Agència determini.

Les instal·lacions i equipament haurà de ser suficient per garantir la continuïtat dels serveis de l'Agència durant l'existència de la causa que doni lloc a la contingència.

3.13 Metodologia, estàndards i lliurables

L'organització del treball i execució del servei s'haurà d'adequar a les metodologies, estàndards i lliurables establerts per l'Agència vigents en el moment de l'execució del servei objecte del contracte basat.

3.14 Seguretat

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

3.11.1. 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, entre altres) 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) 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), 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

L'empresa adjudicatària haurà de presentar un informe de seguiment de cada contracte basat d'acord amb els indicadors de compliment i altra informació rellevant pel seguiment del servei. Aquests informes s'avaluaran als comitès operatius i es formalitzaran i s'elevaran els seus resultats a la resta de comitès.

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

- Un informe de gestió dels serveis desenvolupats per a cada basat, amb indicació de les activitats realitzades i les previstes realitzar, les volumetries globals d'activitat i els indicadors de compliment especificats als Acords de Nivell de Servei (ANS) de cada basat.
- Un informe de dedicació del basat a les diferents funcions requerides, per tal de poder avaluar la distribució dels esforços.
- Un informe d'accions de millora de l'activitat del propi basat, on es detallaran les accions de millora proposades amb informació rellevant per a la seva gestió (per exemple, el benefici previst obtenir, el termini d'implantació). 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.

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), 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.

3.15. Compromís amb el talent i la inclusió

L'Estratègia de la Ciberseguretat de Catalunya 2019-2022, així com la proposta per a la nova Estratègia 2023-2027, reconeixen com un dels seus pilars la generació, captació i conservació de talent. I, és que, en un context d'escassetat de perfils especialitzats en el sector, l'Agència té la voluntat d'impulsar iniciatives que fomentin el desenvolupament de nous professionals e Ciberseguretat. A la vegada, dites estratègies de Ciberseguretat també preveuen com un dels objectius centrals de les polítiques públiques el coneixement i accés de la societat a la comunicació i tecnologies de la informació.

Doncs bé, atenent aquests dos elements l'Agència té el compromís de fomentar la inclusió de persones amb discapacitat dins dels seus programes de talent ja que aquest tipus de perfil aporta un doble valor en la seguretat de les xarxes: (i) permet resoldre conflictes i vulnerabilitats amb perspectives diverses i, per tant, més completa i (ii) assegura que l'objectiu "d'accés" de la ciutadania a les solucions de seguretat sigui total.

Per deixar palès aquest compromís i voluntat, l'Agència preveu en el present contracte criteris per fomentar la inclusió en la generació de talent i la seva presència en el camp de la Ciberseguretat.

La naturalesa d'aquest servei —centrat en el seguiment de l'adequació normativa a l'Esquema Nacional de Seguretat (ENS) dins del sistema sanitari públic— exigeix un alt nivell de precisió metodològica, capacitat analítica, gestió sistemàtica de dades i interacció amb múltiples actors institucionals. En aquest context, la incorporació de talent femení aporta un valor operatiu objectiu que contribueix a la qualitat i l'eficiència del servei per diversos motius concrets:

1. Millora de la representativitat funcional en entorns amb alta presència femenina
El servei es desplega en organitzacions sanitàries públiques, on gran part dels perfils professionals (especialment en àrees d'infermeria, gestió clínica i administració) són majoritàriament femenins. Incorporar talent femení a l'equip del Servei millora l'alineament socioprofessional amb els equips de

les entitats, afavorint una comunicació més fluida, empàtica i operativa durant la recollida i validació d'evidències. Això no és una qüestió d'estil, sinó de coherència funcional amb el context d'implantació del servei.

2. Increment de la qualitat en processos de documentació i traçabilitat
L'execució del servei requereix una gestió documental rigorosa, especialment en la transposició de controls de l'ENS, la definició d'evidències, l'actualització de la matriu de compliment i l'elaboració d'informes de seguiment. Les dades internes de múltiples projectes del sector públic mostren que la diversitat de gènere en equips amb alta càrrega documental millora l'eficiència dels processos de revisió creuada, incrementa la detecció d'errors i afavoreix una millor adaptació dels documents a entorns administratius on la formalització i claredat són imprescindibles.

3. Complementarietat en la governança de solucions tecnològiques corporatives
La solució operativa del servei es basa en SharePoint, PowerAutomate i PowerBI, tecnologies que, segons dades de participació en programes de capacitació TIC en el sector públic català, presenten una creixent presència de talent femení. Això demostra una capacitat instal·lada real que pot ser activada dins l'equip Servei, millorant la sostenibilitat i escalabilitat de la gestió de la solució, especialment en funcions de suport, governança i visualització analítica.

4. Contribució directa a la millora dels indicadors de servei
Diversos indicadors clau del servei (com ara el % d'evidències entregades dins de termini, el % d'evidències validades a la primera, o el grau de satisfacció dels responsables d'entitat) es veuen positivament impactats en equips diversos que combinen perfils tècnics i operatius amb experiència en entorns col·laboratius. En aquest cas, la participació femenina aporta un coneixement operatiu valuós en la interacció amb organitzacions complexes i en la gestió de processos transversals, especialment quan hi ha implicació de múltiples departaments i perfils no TIC.

5. Coherència amb les directrius i recomanacions de bones pràctiques del sector públic
L'impuls a la igualtat d'oportunitats i a la presència de talent femení en l'àmbit tecnològic forma part de les directrius de la Unió Europea, de l'estratègia estatal de digitalització i dels plans d'igualtat en l'àmbit públic. Incorporar aquest criteri de manera efectiva i vinculada a l'operativa del servei, reforça l'alineament institucional i demostra capacitat de desplegament amb criteris de responsabilitat social aplicats a contextos reals i crítics com el sanitari.