Plec de prescripcions tècniques particulars que regeix la contractació basada relativa a serveis de suport per a l'adequació a l'Esquema Nacional de Seguretat (ENS) i el procés de certificació en l'àmbit Sanitari de Catalunya

Exp. CB25AMCONSL1B005

Índex

1 Introducció. 4

1.1 Funcions de l'Agència de Ciberseguretat de Catalunya rellevants a efectes del la nova estratègia de contractació. 5

2 Antecedents. 6

2.1 Objectius generals del model i dels serveis de suport objecte de la licitació. 7

3 Descripció dels serveis objecte de la contractació basada. 8

3.1 Context dels serveis objecte de la licitació i abast. 8

4 Suport per a l'adequació a l'ENS i el procés de certificació. 9

4.1 Funcions i responsabilitats del servei. 9

4.2 Característiques del servei. 12

4.3 Indicadors del Procés de preparació per a l'adequació a l'ENS. 16

4.4 Lliurables del procés de seguiment per a l'adequació a l'ENS 17

5 Condicions d'execució del servei. 20

5.1 Horaris 20

5.2 Localització física. 20

5.3 Equip de treball 20

5.3.1 Perfils 22

5.4 Canvi de recurs 27

5.5 Control de rotació 27

5.6 Eines i equipament per a la prestació de serveis. 27

5.7 Gestió del coneixement 28

5.8 Seguretat Corporativa 29

5.9 Control de Gestió 29

5.10 Documentació. 30

5.11 Formació 30

5.12 Contingència 30

5.13 Metodologia, estàndards i lliurables 31

5.14 Seguretat 31

5.14.1. Deure de confidencialitat. 31

5.14.2. Dades de caràcter personal. 31

5.14.3. Compliment del marc legal de ciberseguretat i del marc normatiu intern. 32

5.14.4. Capacitat tècnica. 32

5.14.5. Adquisició de productes/eines i productes o serveis de seguretat. 32

5.14.6. Interconnexions. 33

5.14.7. Verificació del compliment i auditoria. 33

5.14.8. Incidents de seguretat. 33

5.14.9. Accés a la informació....33
5.15. Assegurament i control de la qualitat i la millora contínua....34
5.16. Seguiment del servei....34
5.17. Integració amb altres equips....35

1 Introducció.

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

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

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

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

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

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

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

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

Avui en dia l'Agència té les següents funcions:

- L'Àrea de Gerència s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació i la gestió de personal.
- Operació de la Seguretat du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció, resposta i recuperació de seguretat en la seva vessant més operativa i la seguretat corporativa.
- Desenvolupament d'Estratègia d'Àmbits té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes i iniciatives de seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- 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 Ciberseguretat de Catalunya, recolza el coneixement, sensibilització i conscienciació, i la innovació com a palanca de transformació i creixement del sector i fomenta la captació de forns i la internacionalització de l'entitat.
- Certificacions en matèria de Ciberseguretat per desplegar totes les eines i processos vinculats al procés de certificació en ciberseguretat de les entitats, garantint sempre la independència necessària per la correcta execució d'aquests processos.

2 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.

L'objecte de la present licitació és la contractació d'un servei de suport per a les entitats de l'àmbit sanitari de Catalunya, orientat a garantir el compliment normatiu en matèria de seguretat de la informació, d'acord amb els requisits de l'Esquema Nacional de Seguretat (ENS) i altres normatives aplicables.

El servei ha de proporcionar suport tècnic i metodològic a les entitats sanitàries en el procés d'adequació a l'ENS i de preparació per a la seva conformitat facilitant el compliment dels requisits, així com durant el procés de certificació o re-certificació. Mitjançant un enfocament sistemàtic i planificat, el servei ha de garantir que les entitats puguin superar amb èxit l'auditoria de certificació i mantenir la conformitat amb la normativa vigent.

A més, i en el cas que no es disposi d'informació prèvia sobre l'estat de situació de l'entitat, el servei ha d'oferir un assessorament inicial per analitzar el nivell de compliment, detectar desviacions i proposar recomanacions específiques. Aquesta diagnosi ha de servir de base per definir un pla d'adequació detallat amb mesures, calendari i responsables.

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 per a l'adequació a l'Esquema Nacional de Seguretat (ENS) i el procés de certificació 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/.

4 Suport per a l'adequació a l'ENS i el procés de certificació.

4.1 Funcions i responsabilitats del servei.

A continuació es descriuen les tasques pròpies del servei:

- **Diagnòstic inicial del grau de compliment**, quan l'entitat no disposi d'informació prèvia, basat en un qüestionari per detectar desviacions de la normativa i **elaboració d'un informe d'avaluació del nivell de compliment de l'ENS**.

- Identificació de les accions d'adequació necessàries i **definició d'un pla d'acció per a l'adequació.**

  Prèviament, el servei donarà suport a la identificació específica dels serveis i sistemes que seran objecte de l'adequació a l'ENS i determinació, d'acord amb l'entitat, de la categorització associada (bàsic, mitjà o alt) o dels perfils de compliment específics de seguretat que estratègicament es defineixin per l'àmbit sanitari.

  El pla d'acció per a l'adequació contindrà, com a mínim, la següent informació:

  - Diagnosi inicial.
  - Accions correctives per les mesures pendents.
  - Responsables d'execució assignats.
  - Terminis estimats.
  - Priorització segons criticitat i dependències.
  - Estat o identificador del nivell d'execució.

  El pla d'acció ha d'estar acompanyat d'una guia que permeti a l'entitat avançar amb certa autonomia durant tot el procés.

- **Suport en l'elaboració de les evidències tècniques i documentals** necessàries per acreditar el compliment de la normativa. En relació amb les evidències documentals, el servei inclourà el suport per a la creació, revisió, adaptació o millora de les plantilles de la documentació essencial, com ara:

  - Política de seguretat de la informació (incloent-t'hi el procediment de gestió de normativa aplicable i model de registre; i la normativa d'ús de mitjans electrònics).
  - Documents d'adequació (informe INES, Categorització del sistema, Declaració d'Aplicabilitat, Anàlisi de riscos, Assumpció de riscos i compromisos de millora, etc.).
  - Procediments de ciberseguretat, com ara, revisió i neteja de metadades no desitjades, adquisició segura d'actius, gestió d'incidents, gestió d'usuaris, còpies de seguretat, entre d'altres.

- **Suport tècnic i metodològic en la gestió, identificació, recollida i anàlisi d'evidències** per acreditar el compliment de la normativa.

Les tasques incloses són, entre d'altres:

- Elaboració de cronograma de treball, si s'escau. En cas que l'entitat tingui diversos sisemes planificats per ser preparats per a la conformitat, el servei coordinarà amb els responsables de l'entitat l'ordre d'actuació, establint una estratègia clara d'aproximació que permeti optimitzar recursos i terminis.

- Elaboració de la matriu de conformitat que inclourà les evidències requerides, la seva descripció i les persones responsables d'aportar-les, amb l'objectiu d'acreditar el compliment dels controls de l'ENS. Aquest document operatiu actuarà com a marc metodològic compartit entre el servei i les entitats, garantint una comprensió clara, homogènia i alineada sobre les evidències a lliurar i les accions necessàries per completar el procés.

- Creació de l'estructura de les carpetes del repositori per a la recopilació i gestió integral de les evidències.

- Assistència als actors implicats en la identificació i el lliurament de les evidències. Així mateix, donarà suport a les entitats en l'elaboració de les evidències i preparació de la documentació que exigeix la normativa objecte de la conformitat.

- Anàlisi qualitatiu i de compliment de les evidències, incloent la validació de la traçabilitat i integritat de les mateixes.

- Elaboració d'informes de seguiment del procés de conformitat.

- **Suport tècnic i metodològic durant el procés de certificació o re-certificació, incloent:**

  - Assistència en la gestió d'accés i ús de l'eina µCeEns del CCN-CERT vetllant perquè la documentació presentada sigui coherent, completa i d'acord amb els criteris d'avaluació oficials, amb:

    - Suport en la sol·licitud i delegació de permisos.

    - Càrrega d'evidències de forma ordenada i segura, revisant-ne la conformitat amb els criteris establerts pel CCN-CERT.

  - Acompanyament durant l'auditoria de certificació, amb suport directe per:

    - Resoldre dubtes de l'auditor i respondre observacions.

    - Preparar documentació addicional en temps real.

    - Donar resposta tècnica a observacions i possibles no conformitats.

  - Elaboració i seguiment del pla d'acció de les accions correctives (PAC) com a resultat de l'auditoria de certificació.

- **Seguiment posterior a l'auditoria**, orientat a la millora contínua i al manteniment de la certificació. Així mateix, el servei també assistirà com a suport expert quan en el seguiment del pla amb les entitats sorgeixin dubtes concrets relacionats amb la preparació per la conformitat en l'ENS de l'entitat i posterior revisió de conformitat i evolució cap a la certificació.

- **Desenvolupament del quadre de comandament estratègic.**

  En col·laboració amb l'equip de Govern de la Dada, el servei haurà de participar activament en el disseny, desenvolupament i manteniment d'un quadre de comandament estratègic, que permeti fer el seguiment global i detallat de l'operativa del servei i de totes les conformitats en curs.

  Aquest quadre de comandament haurà de proporcionar:

  - Indicadors clau (KPIs) sobre el grau de compliment, l'estat de les evidències, els terminis, les iteracions i la qualitat del lliurament.
  - Visualitzacions consolidades i desglossades per entitat, sistema, nivell de seguretat i estat del procés.
  - Visualitzacions consolidades agrupades de totes les entitats del servei per facilitar la presa de decisions i identificar millores.
  - Capacitat d'alerta i detecció de desviacions, per facilitar una gestió proactiva del servei.
  - 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.

Així mateix, formen part de les tasques pròpies del servei la realització de projectes d'evolució i innovació tecnològica del servei mitjançant agents d'intel·ligència artificial.

El servei ha d'incloure de manera obligatòria la **definició, planificació, execució, desplegament i suport a projectes d'evolució del servei**, orientats a incrementar el grau de maduresa, eficiència operativa i capacitat de resposta dels processos de seguretat de la informació de l'organització.

Aquests projectes d'evolució han d'estar basats en l'ús d'agents d'intel·ligència artificial, entesos com a components software capaços de realitzar tasques de manera autònoma o semi autònoma sota supervisió humana. El desplegament efectiu d'aquests projectes constitueix una obligació essencial del contracte, i no tindrà caràcter opcional.

El contractista ha d'adscriure al contracte l'equip tècnic necessari per garantir la correcta execució d'aquests projectes d'evolució, incloent perfils amb experiència en el desenvolupament i l'operació de solucions basades en intel·ligència artificial. L'equip ha de disposar de la capacitació adequada per assegurar la supervisió humana dels agents d'IA, la seva integració amb els sistemes existents a l'Agència i el manteniment durant tota la vigència del contracte.

En tot cas, els projectes d'evolució basats en agents d'IA s'han de desenvolupar d'acord amb els principis i criteris propis de l'Agència, així com els principis d'interoperabilitat, seguretat, auditabilitat i explicabilitat. A la vegada, s'ha de garantir el compliment en tot cas amb els requeriments establerts en la matèria per la Generalitat de Catalunya i l'Agència, així com amb la normativa vigent en matèria de protecció de dades, seguretat de la informació i resta de normativa aplicable. L'abast concret, la priorització i la planificació temporal de cada projecte es definiran durant l'execució del contracte, en coordinació amb l'òrgan responsable del servei.

Aquests agents hauran de ser desenvolupats mitjançant la solució corporativa de l'Agència (COPILOT de Microsoft O365) o la que la pròpia entitat determini, el llicenciament del qual es regirà pels principis establerts en el present plec.

Queden fora de l'abast del servei objecte del present expedient les següents tasques:

- **Realització d'auditories internes formals o anomenades de segona part.** Aquesta funció correspon a l'entitat sanitària pròpiament, o a un tercer especialitzat en dita tipologia d'auditories.

- **Actuacions del Departament de Salut com entitat**, ja que les actuacions en aquest àmbit no s'inclouen en 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 signat entre el Servei Català de la Salut i l'Agència de Ciberseguretat, i 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.

- **Accions d'adequació a l'ENS que comportin despeses** no contemplades en l'operativa ordinària objecte d'aquest plec.

4.2 Característiques del servei.

El servei de suport per a l'adequació a l'ENS es basa en una metodologia pròpia definida per l'Agència, que es recolza en una eina tècnica corporativa dissenyada específicament per a la gestió integral i eficient de les evidències. Aquesta eina (en endavant, el "Sistema"), desenvolupada sobre les plataformes SharePoint, PowerAutomate i PowerBI, actua com a entorn únic per a la recollida, validació i seguiment d'evidències, i la seva utilització és obligatòria i exclusiva per part del Servei adjudicatari durant totes les fases del servei. No es permet la gestió d'evidències mitjançant correu electrònic ni altres canals no controlats.

El Sistema inclou un gestor documental accessible per les entitats, on poden dipositar les evidències requerides, consultar l'estat de validació de cada aportació en temps real i rebre comunicacions a través d'un entorn estructurat i amb traçabilitat. Addicionalment, disposa de mecanismes automatitzats de notificació i recordatori, que faciliten la recollida contínua i ordenada de la documentació necessària.

Aquest Sistema permet una elevada eficiència i un alt grau de paral·lelització en les tasques, ja que optimitza el flux d'informació entre l'entitat i el proveïdor adjudicatari i redueix càrregues administratives innecessàries. D'aquesta manera, l'esforç del servei objecte del present document es pot focalitzar en les activitats de més valor afegit: la revisió rigorosa de les evidències i l'assessorament personalitzat a les entitats durant tot el procés d'adequació i de preparació per a la conformitat en l'ENS. A més, mitjançant indicadors clau visibles en temps real a través de quadres de comandament PowerBI, es pot supervisar l'estat global del servei i prendre decisions informades amb agilitat i transparència.

En relació al Sistema, el servei serà responsable de:

- Gestionar operativament el Sistema, incloent l'alta de noves adequacions, la configuració de l'estructura de carpetes, la gestió dels permisos d'accés i l'activació dels fluxos automatitzats de seguiment i notificació.

- Mantenir, evolucionar i governar el Sistema, adaptant-lo a nous requeriments normatius, funcionals o tècnics, i assegurant-ne el correcte funcionament al llarg del temps.

- Assegurar la integritat i la traçabilitat de la informació, mitjançant l'ús de sistemes automatitzats i registres d'auditoria.

En el cas de la preparació per a la conformitat en el Perfil de Compliment Específic de Requisits Fonamentals de Seguretat (PCE RFS), es disposa d'una altra eina corporativa que permet automatitzar la generació dels resultats del diagnòstic del grau de compliment (indicadors i recomanacions) a partir de la informació continguda en un qüestionari interactiu també en disposició de l'Agència.

A continuació es descriuen algunes de les tasques que ha de dur a terme el servei i que requereixen d'una explicació més detallada:

Creació de l'estructura de carpetes al repositori (SharePoint):

Amb l'objectiu de realitzar una recollida i gestió integral de les evidències s'utilitzarà un repositori ja existent ubicat en els sistemes de Govern de la Dada de l'Agència dissenyat amb aquest propòsit. A tal efecte el servei haurà de realitzar les següents actuacions:

- Donar d'alta el sistema o entitat en la plataforma corporativa habilitada per a la gestió d'evidències (SharePoint).
- Crear l'estructura de carpetes necessària per a la recollida i classificació d'evidències, d'acord amb el model establert, assignant les carpetes segons els responsables departamentals o per unitats administratives.
- Coordinar-se amb el responsable de l'entitat sanitària per donar les indicacions pertinents per iniciar la recollida d'evidències. També s'encarregarà de gestionar els permisos d'accés per als diferents actors implicats de cada entitat, assegurant que només hi accedeixin els perfils autoritzats.
- Verificar que els fluxos automatitzats implementats al repositori (recordatoris, notificacions, etiquetatge automàtic) estiguin plenament operatius i adaptats al servei.

Sessió kick-off d'explicació del model de preparació per a l'adequació a l'ENS**:**

- El servei serà responsable de convocar, quan sigui necessari, una reunió inicial amb tots els actors implicats de cada entitat, validant prèviament la disponibilitat dels assistents i assegurant la seva participació activa. Si es considera adient i amb l'objectiu d'aprofitar sinergies, es podrà convocar una reunió conjunta que agrupi diverses entitats.
- Coordinar aquesta sessió amb el servei de Governança que coordina i fa el seguiment dels plans de seguretat per assegurar l'alineament.
- Aquesta sessió té com a objectiu garantir una comprensió homogènia del model d'adequació i preparació per a la conformitat en l'ENS, els objectius temporals, els rols i les responsabilitats.
- Haurà de revisar i, si cal, actualitzar el material de presentació per tal que reflecteixi el context i les característiques específiques del servei en qüestió.
- Durant la sessió, es realitzarà una explicació detallada del procés, les eines que s'utilitzaran (com SharePoint i µCeEns), les fites previstes i les possibles incidències que cal anticipar.

Sol·licitud del llistat d'evidències:

- El servei haurà de confeccionar el llistat d'evidències requerides per a la preparació per la conformitat en l'ENS del servei, adaptat a l'àmbit funcional i la categorització o el perfil de compliment específic de seguretat corresponent.
- Les evidències d'aquest llistat s'hauran de classificar segons la seva naturalesa: evidències específiques del servei, evidències específiques del sistema associat, evidències transversals de l'entitat, etc.
- Un cop validat internament, el servei haurà d'enviar el llistat a cada actor responsable de l'entrega de les evidències, indicant-hi les instruccions per a la seva generació o recuperació.

Seguiment del lliurament d'evidències:

- El servei haurà de dur a terme un seguiment actiu del lliurament d'evidències, revisant periòdicament l'estat de les carpetes al repositori, i informarà als responsables de les entitats un resum setmanal amb els principals canvis esdevinguts.
- En cas de detectar evidències pendents o incorrectes, haurà d'enviar comunicacions de recordatori als responsables, amb el detall de les mancances i la seva afectació en el procés. Proporcionarà el suport necessari a les entitats per corregir-les.
- Quan per volumetria de les entitats es consideri adient, s'activarà un sistema automatitzat de recordatoris (bot) que permetrà fer el seguiment i traçabilitat de les notificacions emeses, permetent establir un màxim d'iteracions predefinides per entitat.

Validació de recepció de l'evidència sol·licitada:

- Cada vegada que es detecti una nova evidència carregada al repositori, el servei haurà de verificar la seva integritat (format, data i ubicació).
- En cas que sigui correcta, s'enviarà un correu de confirmació de recepció a l'actor responsable, deixant traça de la gestió.

Anàlisi de l'evidència:

- El servei haurà de revisar en detall cadascuna de les evidències lliurades, contrastant-les amb els requisits establerts pel CCN-CERT i el nivell de seguretat exigit.
- Quan una evidència sigui insuficient o incorrecta s'informarà al responsable de l'entitat, tot indicant quins són els aspectes a corregir per a la seva reformulació o substitució.
- El servei haurà d'identificar aquelles evidències que les entitats tenen més dificultats per generar o interpretar i que, en conseqüència, solen resultar incompletes o inadequades, així com proposar les millores necessàries per corregir aquesta situació.

  A nivell estimatiu, durant l'any 2025 es van analitzar 4.063 evidències.

Comunicació de l'anàlisi d'evidències (BOT automàtic):

- El servei haurà de configurar i gestionar un sistema automatitzat de comunicació que informi als actors implicats dels resultats de l'anàlisi, així com dels següents passos requerits.

Preparació de l'entorn del µCeEns:

- El servei assessorà en la sol·licitud d'accés de l'entitat a l'eina µCeEns.
- També proporcionarà acompanyament tècnic per completar els formularis i qüestionaris de l'eina µCeEns, garantint la coherència de les dades introduïdes.
- Serà responsabilitat del servei descarregar les evidències aprovades del repositori i realitzar-ne la càrrega a µCeEns, sempre que disposi de l'accés delegat corresponent.

Documents del procés de preparació per a la conformitat en l'ENS:

- **Categorització de sistemes:**
  - El servei donarà suport a l'entitat en l'elaboració del document de categorització del sistema segons les dades de l'entitat i el servei, ajustant-se a la normativa aplicable. Aquest document serà validat i signat oficialment per la figura corresponent de l'entitat.
- **Anàlisi de Riscos:**
  - A partir de la informació recopilada, l'entitat durà a terme l'anàlisi de riscos. El servei verificarà que aquest procés s'ha realitzat d'acord amb les directrius de l'ENS. Aquest document serà validat i signat oficialment per la figura corresponent de l'entitat.
- **Declaració d'aplicabilitat:**
  - El servei donarà suport a l'entitat en l'elaboració del document de declaració d'aplicabilitat amb la informació del servei objecte de la preparació per a la conformitat.

Certificació de conformitat en l'ENS:

- El servei haurà de realitzar una revisió integral de totes les evidències i documentació carregada, assegurant que compleixen els requisits per a iniciar el procés de certificació.
- Posteriorment, gestionarà la sol·licitud formal d'auditoria a través de la plataforma µCeEns.
- Iniciat el procés de certificació, oferirà suport en la resolució de dubtes que pugui tenir l'OAT de l'Agència i facilitarà qualsevol informació addicional requerida.
- Un cop finalitzada l'auditoria, també elaborarà i farà el seguiment del pla d'acció de les accions correctives (PAC) com a resultat de l'auditoria de certificació
- Finalment, el servei gestionarà el tancament del procés de conformitat en l'ENS, confirmant l'obtenció de la certificació per part de l'entitat.

Les tasques pròpies del servei es duran a terme en col·laboració i coordinació estreta i efectiva entre totes les parts implicades per assolir els objectius establerts. Principalment,

- actors implicats de les entitats, per el lliurament de les evidències.
- equip tècnic dels prestadors de servei de les entitats, per el lliurament de les evidències.
- serveis de l'Agència:
  - Servei de Governança, per compartir la planificació, els resultats obtinguts, els contactes dels actors de les entitats involucrats i tota la informació necessària dels sistemes d'informació dins l'abast.

- Òrgan d'Auditoria Tècnica (OAT), per l'execució del procés de certificació.

El servei ha d'observar els següents elements essencials:

- Implementació de processos, metodologies i formes de treball creatives i innovadores que permetin impulsar i assessorar el compliment de les normatives de manera ràpida i eficient per aconseguir el propòsit d'estar preparades per a la conformitat en el mínim temps i esforç possible, optimitzant els processos.
- Reducció de l'esforç manual mitjançant eines que permetin optimitzar el temps dedicat a cadascuna de les tasques, millorant la seva eficiència i escalabilitat i automatitzant al màxim les diferents accions, tasques i lliurables plantejats.
- Disseny i execució d'actuacions grupals que puguin ajudar a donar un impuls a les certificacions o quan hi hagi canvis que afectin a totes les entitats a nivell d'evidències, enfocs, etc. Addicionalment, coordinarà i impartirà formacions grupals per assessorar i guiar a les entitats. Això també pot aplicar-se a metodologies que internament es defineixin, plantilles d'ús comú, etc.

4.3 Indicadors del Procés de preparació per a l'adequació a l'ENS.

En el marc del servei, el seguiment mitjançant indicadors clau (KPIs) és essencial per garantir la qualitat, eficiència i traçabilitat de les actuacions. Aquests indicadors han de ser gestionats pel servei, que tindrà la responsabilitat de generar, mantenir i evolucionar-los al llarg de tot el projecte.

A continuació es proposen els següents indicadors que permeten avaluar tant el progrés operatiu com l'impacte dels lliuraments i la satisfacció dels actors implicats. A més, la incorporació de models visuals facilitarà la presa de decisions i la identificació proactiva de possibles desviacions.

El servei podrà proposar altres mètriques i indicadors del servei, inclosos els de seguiment operatiu.

Indicador	**Responsabilitat del Servei**
% de sistemes identificats i categoritzats	Ha de registrar, mantenir i validar que tots els sistemes tinguin el seu nivell de compliment documentat correctament de forma global i per entitat.
Temps mitjà de preparació per a la conformitat per sistema (dies)	Caldrà monitorar els temps entre l'inici de l'anàlisi i la fi de la preparació per a la conformitat en l'ENS, identificant desviacions respecte al cronograma inicial per ajustar planificacions futures.
% d'evidències entregades dins del termini establert al cronograma inicial	Gestionarà el control de lliurament d'evidències respecte als terminis, activant alertes si cal.
Volumetria d'evidències gestionades pel servei i per entitat mensuals	Permetrà quantificar el volum real d'activitat. Aquesta informació és essencial per calibrar la capacitat operativa
Volumetria d'evidències revisades mensuals	Volumetria d'evidències:

	Evidències rebudes, Evidències revisades separant quines s'han considerat adequades i quines no.
% d'evidències validades a la primera revisió	Detectarà problemes de qualitat o maduresa en la sol·licitud d'evidències i realitzarà millores si el % és baix.
Temps mitjà entre anàlisi d'evidència i comunicació de resultats	Mesurarà el temps de resposta i realitzarà millores si és baix.
% d'evidències correctament pujades a µCeEns	Controlarà el traspàs final de les evidències i en registrarà errors o omissions detectades pel sistema.
% de sistemes amb els documents requerits per a la conformitat signats dins del termini segons el cronograma inicial	Assegurarà l'elaboració i seguiment dels documents fins a la seva validació i signatura institucional.
% de serveis que obtenen la certificació sense observacions	Analitzarà els informes d'auditoria per avaluar la qualitat del procés previ a la certificació.
% temps del procés	Temps mig per tipologia d'entitats que estan trigant des de que es comencen a pujar evidències fins que: • S'inicia el tràmit al µCeENS. • Fins que es sol·licita l'auditoria a través de l'eina µCeENS.
Satisfacció dels responsables d'entitat (enquesta NPS)	Dissenyarà, enviarà i analitzarà l'enquesta de satisfacció, extraient conclusions per a la millora contínua.

4.4 Lliurables del procés de seguiment per a l'adequació a l'ENS

En el marc del procés de seguiment per a l'adequació a l'ENS, el servei tindrà la responsabilitat de generar, mantenir i lliurar un conjunt estructurat de lliurables que permetin garantir la correcta supervisió de les accions realitzades.

Aquests lliurables constitueixen una eina clau per verificar el grau de compliment dels requisits normatius, assegurar la traçabilitat de les evidències i facilitar la presa de decisions basada en dades objectives. A més, permeten una comunicació fluida amb tots els actors implicats i una avaluació contínua de l'estat del servei.

Tots els documents i productes associats al seguiment hauran de ser presentats dins els terminis establerts, amb el nivell de qualitat i rigor requerit, i estaran subjectes a revisió i validació per part de l'Agència i les entitats.

A continuació es detallen els principals lliurables que el Servei haurà de lliurar:

1. **Diagnòstic** i **informe d'avaluació del grau del nivell de compliment de l'ENS**.
2. **Document d'identificació del servei, sistema i, categorització i tipus de conformitat objectiu.** Aquest document ofereix a l'equip auditor una visió general del sistema d'informació dins l'abast de l'auditoria. S'hi descriuen els serveis d'informació i la tecnologia que els suporta, amb l'objectiu de facilitar la comprensió del context i identificar els principals components tecnològics implicats.
    - Identificació del servei, sistema d'informació i tecnologia associada.
    - Visió general del sistema d'informació i la tecnologia.
    - Tipus de conformitat: Categoria del sistema (bàsica, mitjana o alta) o perfil de compliment específic.
3. **Pla d'acció i cronograma de treball de les accions** necessàries per a l'adequació a l'ENS.
    - Fites, objectius temporals i rols responsables.
    - Eina fonamental per al seguiment temporal del projecte.
4. **Matriu de conformitat amb les evidències i els responsables del lliurament.**

    Aquesta matriu haurà d'incloure:
    - La relació completa i actualitzada dels controls de seguretat de l'ENS.
    - La descripció de les evidències específiques que cal aportar per a cada control, segons el perfil i nivell de compliment requerit.
    - Exemples concrets i orientatius d'evidències vàlides, per facilitar a les entitats la comprensió del que s'espera lliurar.
    - La vinculació entre controls, evidències i responsabilitats internes de l'entitat, per garantir una gestió col·laborativa i eficient.
5. **Plantilles d'evidències tècniques i documentals**.
6. **Informe de seguiment del lliurament d'evidències.**
7. **Informe d'avaluació del grau de compliment.**
8. **Materials necessaris per al correcte desenvolupament del servei.** Entre d'altres,
    - Presentacions de la sessió de kick-off, tancament o altres reunions.
    - Presentacions executives sobre el seguiment del lliurament d'evidències i el grau de compliment.
    - Pla de capacitació interna, materials formatius i identificació de formacions.

- Documentació tipus o de suport dirigida als equips interns i als àmbits (guies, manuals, plantilles, etc.).

9. **Plans d'acció de les accions correctives** com a resultat de l'auditoria de certificació **(PAC).**
10. **Informe de Satisfacció i Millora Contínua.**
    - Recull de feedback de les entitats amb proposta de millores per futurs processos.

5 Condicions d'execució del servei.

5.1 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.

5.2 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 puntual 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.

5.3 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\Coordinador/a**. Aquesta figura haurà d'assumir-la el membre de l'equip amb més experiència, que alhora compleixi amb un dels perfils de consultor/a descrits més endavant. És a dir, **no s'ha d'incloure un perfil específic de Cap de Servei\Coordinador/a del servei**, sinó que aquestes funcions s'assignaran a un dels membres de l'equip requerit, sense perjudici de les seves responsabilitats pròpies. A aquest efecte, ha de assumir les següents responsabilitats:

- 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.
- Garantir que l'Agència rebi els informes de gestió acordats i realitzar el seguiment econòmic i d'activitat amb els interlocutors de l'Agència.
- Proposar, generar, implementar, mantenir i calcular les mètriques i els indicadors del servei, inclosos els de seguiment operatiu que siguin adequats per tal de reportar als responsables de l'Agència i les entitats.
- Realitzar el seguiment dels indicadors i informes de progrés,
- Generar 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.
- Garantir que els lliurables realitzats s'entreguen a l'Agència en forma i qualitat esperats.
- Gestionar les altes i les baixes del personal de l'adjudicatari conforme els protocols de l'Agència.
- Planificar, coordinar, supervisar i avaluar totes les activitats necessàries per a l'operativa del servei.
- Coordinar amb la resta d'àrees i equips de l'Agència assegurant una bona col·laboració entre els diferents agents implicats.
- Mantenir la relació amb les entitats.
- Gestionar i donar 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.
- Controlar la qualitat i traçabilitat.
- Gestionar i reportar els riscos operatius del servei.
- Vetllar per la millora contínua del servei.
- Gestionar i coordinar de forma eficient els recursos humans i tecnològics.

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

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

S'estima un total de 1.760 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:

Hores anuals: 10.560 hores.

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

Perfil	Hores anuals estimades
Consultor/a amb expertesa en l'Esquema Nacional de Seguretat superior a 5 anys	**7.040 hores**
Consultor/a amb expertesa en l'Esquema Nacional de Seguretat superior a 3 anys	**1.760 hores**
Consultor/a amb expertesa en l'Esquema Nacional de Seguretat i elaboració de marcs normatius superior a 5 anys	**1.760 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** són: **13.200 hores.**

5.3.1 Perfils

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

PERFIL	REQUISITS
Consultor/a amb expertesa en l'Esquema Nacional de Seguretat superior a 5 anys	**Formació acadèmica:** • Grau o enginyeria en Informàtica, Telecomunicacions, Ciències de la Computació o similars en l'àmbit TI. **Certificacions professionals:** • ISO/IEC 27001 (Lead Implementer o Lead Auditor). **Experiència professional:** Experiència professional mínima de 5 anys en projectes de seguretat i adequació normativa. Haver participat i poder demostrar la seva implicació en projectes en els que hagi desenvolupat les següents funcions: • Lideratge de projectes i equips de treball multidisciplinaris. • Projectes amb administracions públiques o entorns regulats. • Gestió de projectes de seguretat, principalment d'adequació i implantació de l'ENS o altres esquemes de seguretat regulats. • Auditoria (en base a metodologia CCN-CERT, ISO27001 o metodologies similars), anàlisi de riscos (en base a metodologia CCN-CERT, ISO27005 o metodologies similars) i proposta de plans d'acció. • Ús i configuració de plataformes corporatives Microsoft 365 (SharePoint, PowerAutomate i PowerBI), aplicades a entorns de gestió documental i fluxos de treball. • Elaboració d'informes executius, incloent la definició i implantació de quadres de comandament, els quals incorporen visions estratègiques, operatives i tàctiques. • 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. **Coneixement en:** • Definició de projectes (metodologies, processos, eines, lliurables, etc.). • Coneixement avançat de l'entorn normatiu, regulatori i models de gestió que apliquen a la ciberseguretat: ENS, ISO 27001, ISO 22301, ISO 22005, RGPD/LOPDGDD, estàndards del CCN-CERT i altres normatives de ciberseguretat o similars. • Coneixement de l'entorn tecnològic (desenvolupament, gestió de serveis TIC, xarxes, gestió de proveïdors, etc.). • Eines Microsoft 365 (SharePoint, PowerAutomate i PowerBI).

	• Eines de generació i presentació d'informació per fer més eficient la comunicació i presa de decisions. **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.
Consultor/a amb expertesa en l'Esquema Nacional de Seguretat superior a 3 anys	**Formació acadèmica:** • Grau o enginyeria en Informàtica, Telecomunicacions, Ciències de la Computació o similars en l'àmbit TI. **Certificacions professionals:** o ISO/IEC 27001 (Lead Implementer o Lead Auditor). **Experiència professional:** Experiència professional mínima de 3 anys en projectes de seguretat i adequació normativa. Haver participat i poder demostrar la seva implicació en projectes en els que hagi desenvolupat les següents funcions: • Projectes amb administracions públiques o entorns regulats. • Projectes de seguretat, principalment d'adequació i implantació de l'ENS o altres esquemes de seguretat regulats. • Auditoria (en base a metodologia CCN-CERT, ISO27001 o metodologies similars), anàlisi de riscos (en base a metodologia CCN-CERT, ISO27005 o metodologies similars) i proposta de plans d'acció. • Ús i configuració de plataformes corporatives Microsoft 365 (SharePoint, PowerAutomate i PowerBI), aplicades a entorns de gestió documental i fluxos de treball. • Definició, implantació i automatització d'indicadors de servei, especialment en l'àmbit de la ciberseguretat. **Coneixement en:** • Coneixement avançat de l'entorn normatiu, regulatori i models de gestió que apliquen a la ciberseguretat: ENS, ISO 27001, ISO 22301, ISO 22005, RGPD/LOPDGDD, estàndards del CCN-CERT i altres normatives de ciberseguretat o similars.

	• Coneixement de l'entorn tecnològic (desenvolupament, gestió de serveis TIC, xarxes, gestió de proveïdors, etc.). • Eines Microsoft 365 (SharePoint, PowerAutomate i PowerBI). • Eines de generació i presentació d'informació per fer més eficient la comunicació i presa de decisions. **Habilitats/Capacitats:** • 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.
Consultor/a amb expertesa en l'Esquema Nacional de Seguretat i elaboració de marcs normatius superior a 5 anys	**Formació acadèmica:** • Grau o enginyeria en Informàtica, Telecomunicacions, Ciències de la Computació o similars en l'àmbit TI. **Certificacions professionals:** • ISO27001 Lead Implementer o ISO27001 Lead Auditor. **Experiència professional:** Experiència professional mínima de 5 anys en projectes de seguretat i elaboració de marcs normatius. Haver participat i poder demostrar la seva implicació en projectes en els que hagi desenvolupat les següents funcions: • Lideratge de projectes i equips de treball multidisciplinaris. • Projectes amb administracions públiques o entorns regulats. • Creació, redacció i manteniment de marcs normatius de seguretat alineats amb l'ENS i ISO 27001 (polítiques, procediments, normatives internes i guies). • Adaptació de requisits normatius a la realitat operativa d'una entitat pública o privada. • Definició de models documentals homogenis, aplicables a diverses entitats o serveis, consistents i auditables. • Col·laboració amb responsables legals i tècnics per garantir que la documentació és jurídicament sòlida i tècnicament viable. • Projectes d'adequació al ENS amb responsabilitat en la generació de documentació formal (Declaració d'Aplicabilitat, Anàlisi de Riscos, Categorització de Sistemes d'Informació, etc.).

	• Suport a auditories internes i externes (en base a metodologia CCN-CERT, ISO27001 o metodologies similars), aportant evidències normatives i justificació de controls. • 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 l'entorn normatiu, regulatori i models de gestió que apliquen a la ciberseguretat: ENS, ISO 27001, ISO 22301, ISO 22005, RGPD/LOPDGDD, estàndards del CCN-CERT i altres normatives de ciberseguretat o similars. • Coneixement de l'entorn tecnològic (desenvolupament, gestió de serveis TIC, xarxes, gestió de proveïdors, etc.). • Principals vulnerabilitats i defectes a les que poden estar subjectes infraestructures, plataformes i aplicacions, així com les propostes de mitigació cost/efectivitat més adients. • Eines de generació i presentació d'informació per fer més eficient la comunicació i presa de decisions. **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. • Capacitat de redacció i síntesi, adaptant llenguatge tècnic i normatiu a formats comprensibles per diferents actors. • Coneixement en estàndards i bones pràctiques relatives al govern de la seguretat de la informació, arquitectura de seguretat i operacions de seguretat.

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

5.4 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.

5.5 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. .

5.6 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

5.7 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions, es requereix que l'empresa adjudicatària registri tot el coneixement que disposi i es generi en l'execució del servei d'acord amb les directrius de l'Agència.

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.

5.8 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.
- 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, LOPD/GDD, 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.

5.9 Control de Gestió

L'empresa adjudicatària del contracte, 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.

5.10 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 el 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.

5.11 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.

- Esquema Nacional de Seguretat (ENS) i els perfils de compliment específics (PCE RFS, PCE Salut, PCE Justícia, etc.), així com altres marcs normatius de ciberseguretat.

- Formació en aspectes tècnics relacionats amb els serveis objectes d'aquest contracte.

Així mateix, ha de dur a terme les 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.

5.12 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.

5.13 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.

5.14 Seguretat

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

5.14.1. 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.

5.14.2. 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.

5.14.3. 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.

5.14.4. 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.

5.14.5. 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, 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.

5.14.6. 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.

5.14.7. 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.

5.14.8. 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.

5.14.9. 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) 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.

5.15. 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), 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.

5.16. 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.

5.17. 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), ja sigui amb l'Agència com directament amb altres Serveis.
- 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.

