Plec de prescripcions tècniques particulars que regeix la contractació d'un servei per al desenvolupament dels mòduls d'operació, d'avaluació i d'adequació normativa de la Plataforma de suport a la governança de la ciberseguretat als àmbits

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Índex

1 Introducció

1.1 L'Agència de Ciberseguretat de Catalunya

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 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 2024, l'entitat ha tingut un paper rellevant en les tasques de resposta i coordinació per a la gestió d'incidents de seguretat durant el 2024, 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 2024 va ser de més de 6.900 milions, en contraposició als 5.000 milions d'atacs del 2023. Pel que fa als incidents de seguretat, l'Agència en va gestionar prop de 3.372 durant el 2024, en comparació amb els 2.665 de l'exercici anterior.

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

1.2 Programa RETECH

Aquest contracte està finançat per fons europeus. El programa RETECH constitueix un dels nous eixos transversals de l'Agenda España Digital 2026 promoguts pel Ministerio de Asuntos Económicos y Transformación Digital, i està alineat amb dues de les principals fites de l'Agenda, com són, liderar la transformació digital de manera inclusiva i sostenible i focalitzar els esforços de digitalització en sectors econòmics clau. L'objectiu del Programa RETECH és impulsar xarxes territorials d'especialització tecnològica, articulant projectes regionals que s'orientin a la transformació i especialització digital, assegurant la coordinació, la col·laboració i la complementarietat.

Gràcies a aquest nou eix de l'Agenda España Digital 2026, es pretén liderar un canvi disruptiu, de manera inclusiva i sostenible, focalitzant els esforços de digitalització en sectors econòmics clau. En definitiva, la iniciativa RETECH permetrà impulsar els projectes tractors proposats per les Comunitats i Ciutats Autònomes, fomentant l' intercanvi de coneixement i multiplicant les oportunitats de cada regió, a través de xarxes d' impacte nacional que permetin maximitzar l'equilibri territorial i la cohesió social entre elles.

Una de les línies d'actuació és RETECH Ciberseguretat, que pretén posar en marxa una estratègia per desenvolupar un ecosistema de ciberseguretat, millorant les capacitats, la indústria, el talent i la recerca, desenvolupament i innovació (R+D+I).

El projecte forma part del marc del Pla de Recuperació, Transformació i Resiliència (PRTR) i compta amb el cofinançament de les comunitats autònomes i dels fons Next Generation de la Unió Europea, la finalitat del qual és contribuir a impulsar i enfortir l'ecosistema de la nacional a la generació de capacitats especialitzades i al treball en xarxa de diferents nodes de ciberseguretat regionals, contribuint per tant a les fites i objectius del PRTR a la temàtica de ciberseguretat, a través del component 15.I7 i els objectius CID relacionats (CID 248).

Per fer efectiva la iniciativa RETECH amb total transparència i igualtat d'oportunitats per a totes les Comunitats i Ciutats Autònomes interessades, el Ministerio de Asuntos Económicos i Transformación Digital, a través de la Secretaria d'Estado de Digitalización e Inteligencia Artificial, va llançar una invitació pública destinada al desenvolupament de propostes de cooperació per finançar iniciatives emblemàtiques d'especialització territorial tecnològica dins de les seves competències.

Hi participen 15 comunitats autònomes articulades en tres nodes que sumen un pressupost inicial de 149 milions d'euros. Les regions participants i els seus ecosistemes respectius formaran part de la Comunitat Nacional Espanyola del Centre Europeu de Competència en Ciberseguretat. En aquest organisme, l'Institut Nacional de Ciberseguretat d'Espanya (INCIBE) actua com a Centre de Coordinació Nacional (NCC-ES).

L'Agència, conjuntament amb l'Agència per a la Modernització Tecnològica de Galícia i la Direcció General de Tecnologies de la Informació i les Comunicacions de la Conselleria d'Hisenda i el model econòmic de la Generalitat Valenciana, proposa desplegar un Centre d'Innovació i Competència en l'àmbit de la ciberseguretat de caràcter interregional.

Objectius del Centre d'Innovació i Competència en Ciberseguretat:

- Cohesionar l'ecosistema de la ciberseguretat a l'estat espanyol.
- Fomentar la capacitació especialitzada en ciberseguretat.
- Impulsar projectes innovadors, solucions i serveis avançats.
- Promoure el creixement de noves empreses en els àmbits del transport intel·ligent, ciències de la salut, indústria connectada i excel·lència operativa.

L'Agència s'encarregarà d'impulsar els sectors estratègics de Ciències de la Salut i Excel·lència Operativa dins d'aquesta iniciativa i per fer-ho compta amb un pressupost de 20 milions d'euros. Les accions que s'executaran s'estructuren en quatre línies d'actuació: cultura i ciberseguretat, desenvolupament d'ecosistemes d'innovació, suport a empreses emergents, i desplegament, desenvolupament i suport a l'adquisició de solucions i serveis.

1.3 Centre DemoTEC

Amb l'aportació dels fons RETECH, el Centre de Competències i d'Innovació (CCI) de l'Agència impulsa el desenvolupament del Centre DemoTEC, una iniciativa impulsada orientada a la recerca aplicada i a la demostració de tecnologies emergents amb alt potencial transformador. El projecte se centra en àrees estratègiques com la computació quàntica, la intel·ligència artificial (IA), la *Robotic Process Automation* (RPA), l'analítica avançada i el *blockchain*, amb l'objectiu d'anticipar els reptes futurs i enfortir les capacitats del país en matèria de protecció digital.

Una de les iniciatives a desenvolupar en el marc del Centre DemoTEC és la Plataforma de suport a la governança de la ciberseguretat als àmbits, concebuda per donar resposta a la necessitat d'una gestió escalable, coordinada i basada en dades de la ciberseguretat dels diferents àmbits d'actuació de l'Agència.

La Plataforma s'estructura en tres blocs principals que es descriuen en el següent apartat: la web del Portal de Seguretat, tres mòduls funcionals integrats i una font de dades de ciberseguretat a nivell de país. Aquesta arquitectura modular ha de garantir construir un entorn interoperable, coherent i escalable, preparat per automatitzar, optimitzar i ampliar els serveis que l'Agència ofereix a les entitats. Addicionalment, i com a element central, la Plataforma incorpora el Quadre de Comandament Integral de Ciberseguretat (QCIC). El QCIC ha de permetre desenvolupar nous models de governança basats en dades, amb capacitat d'escalat, reutilització i intercanvi de dades, consolidant així una visió compartida i orientada a resultats.

En conjunt, la Plataforma ha de possibilitar una gestió eficient, proactiva i basada en dades de la ciberseguretat en els àmbits d'actuació de l'Agència, la qual ha d'impulsar la transformació digital del servei públic de ciberseguretat a través d'un model de governança estratègic, centralitzat i col·laboratiu.

1.3.1 Plataforma de suport a la governança de la ciberseguretat als àmbits

L'Agència impulsa el desenvolupament de la Plataforma de suport a la governança de la ciberseguretat en els seus àmbits d'actuació. Actualment, aquests consten de:

- Generalitat de Catalunya
- Hospitals, centres sociosanitaris i primària
- Administracions Locals
- Universitats

La Plataforma consta del Portal de Seguretat (web), tres mòduls funcionals integrats en aquest portal, i una font de dades de ciberseguretat a nivell de Catalunya. Cada bloc compleix un objectiu específic i diferenciat, però han de funcionar de manera coordinada i interoperable per assolir una gestió estructurada de la ciberseguretat als àmbits d'actuació de l'Agència.

A continuació es descriuen els diferents blocs per tal d'oferir una visió global de la Plataforma, però el present Plec està destinat únicament a la contractació dels mòduls funcionals:

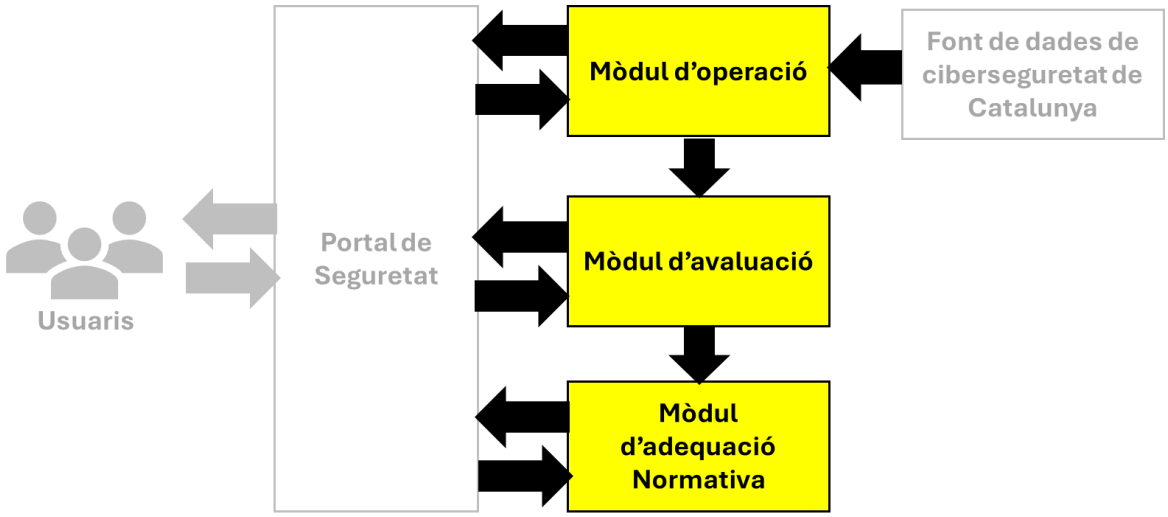
1. Portal de Seguretat (exclòs del present Plec)
    - Portal web per a l'accés centralitzat als serveis de ciberseguretat que ofereix l'Agència a les entitats dels seus àmbits d'actuació.
    - Té com a objectiu consolidar els serveis actualment distribuïts en diversos entorns en un únic accés web, unificat, escalable i orientat a l'usuari, que millori l'accessibilitat, la usabilitat i la coherència dels serveis prestats, de manera que permeti la visualització i entrada de dades necessàries per als mòduls funcionals.
    - Actua com a interfície principal per als usuaris de les entitats dels àmbits d'actuació de l'Agència, facilitant l'accés a recursos, eines, processos i informació rellevant en matèria de ciberseguretat. Garantir una experiència homogènia i optimitzada, tant per a les administracions públiques com per a futurs perfils d'usuari, reforçant la visibilitat i l'eficiència de les accions de l'Agència.
2. Mòduls funcionals (objecte del present Plec)
    - Mòdul d'Operacions (Lot 1 del present Plec)

- Base de dades centralitzada per a la gestió i explotació en quasi temps real, de dades estructurades, semiestructurades i no estructurades de l'activitat operativa de l'Agència en matèria de ciberseguretat.
- Té com a objectiu consolidar les dades operatives de l'Agència en una infraestructura per capes comuna, optimitzant la seva gestió i explotació garantint-ne la disponibilitat, la qualitat i la traçabilitat i de forma integrada amb els sistemes existents i el Portal de Seguretat. Inclou el desenvolupament del QCIC, el quadre de comandament central per a la visualització dels indicadors generats a partir de les dades.
- Aquest mòdul gestiona tot el cicle de vida de les dades operatives de l'Agència: ingesta, transformació i visualització. Permet integrar diferents fonts de dades disperses, estructurar-les segons els processos de l'Agència, i posar-les a disposició dels serveis interns a través de canals d'accés com API, els quadres de comandament del QCIC i eines d'ingesta de dades integrades al Portal de Seguretat. Es tracta de la base de dades central que concentri les mètriques dels serveis i processos de l'organització, inclosos els Mòduls d'Avaluació i d'Adequació Normativa, facilitant una gestió central, àgil i escalable.

- Mòdul d'Avaluació (Lot 2 del present Plec)
  - Solució per avaluar el grau de compliment dels marcs normatius de ciberseguretat aplicables a les entitats dels àmbits de l'Agència.
  - Té com a objectiu oferir un sistema estructurat i eficient que permeti a les entitats avaluar la seva situació en relació amb els requisits de ciberseguretat, identificar àrees de millora i establir plans d'acció per reforçar la seva postura de ciberseguretat.
  - Aquest mòdul disposa al Portal de Seguretat un seguit de qüestionaris personalitzats segons el marc normatiu aplicable a cada entitat, amb preguntes organitzades en subdominis temàtics i estructurades en forma d'arbre lògic. Permet la ingesta i gestió centralitzada de les respostes, l'automatització del càlcul d'indicadors i la generació de resultats clars que serveixen de guia per a l'acció. D'aquesta manera, facilita l'estandardització i escalat del model d'avaluació a un gran nombre d'entitats.
- Mòdul d'Adequació Normativa (Lot 3 del present Plec)
  - Solució per facilitar el procés d'adequació i preparació de les entitats per a la certificació en marcs de ciberseguretat, especialment l'ENS a partir de la recollida d'evidències.
  - Té com a objectiu acompanyar les entitats en les tasques prèvies a una auditoria, simplificant la preparació documental i assegurant que es disposi de totes les evidències necessàries per acreditar el compliment normatiu.
  - Aquest mòdul permet estructurar i gestionar de manera eficient la recollida d'evidències i la documentació associada als requisits de ciberseguretat. Fa ús de tècniques d'intel·ligència artificial per validar automàticament la qualitat i adequació de les evidències recollides, facilitant-ne l'aprofitament en els processos de preparació per a l'obtenció de certificacions. Aquesta automatització permet estandarditzar el procés, reduir errors i descarregar les entitats de tasques manuals repetitives, garantint una preparació més eficient i fiable.

3. Font de dades de ciberseguretat de Catalunya (exclòs del present Plec):
   - Eina per a la captura massiva d'evidències i la monitorització contínua del nivell de ciberseguretat al territori de Catalunya i a les seves entitats.

- Té com a objectiu dotar l'Agència de la capacitat per mesurar de manera objectiva, automatitzada i continuada l'estat de ciberseguretat de les xarxes del país, mitjançant la recollida, anàlisi i consolidació d'evidències provinents d'Internet vinculades a factors de risc i vulnerabilitat.
- Aquesta eina recull de forma massiva indicadors externs com vulnerabilitats exposades, configuracions insegures o senyals d'infecció amb *malware*. A partir d'aquest conjunt de troballes de ciberseguretat, calcula de manera sistemàtica el nivell de ciberseguretat de les entitats públiques en què opera l'Agència. El càlcul es basa en algoritmes objectius i indicadors fiables, i s'actualitza de manera continuada. La solució permet consultar mètriques i evidències de forma estructurada a través del Portal de Seguretat, així com integrar-les automàticament amb altres sistemes d'informació de l'Agència per reforçar la capacitat de seguiment i resposta en tot el territori.



– Diagrama de blocs de la Plataforma de suport a la governança de la ciberseguretat –

En conjunt, la Plataforma de suport a la governança ha de permetre automatitzar, escalar i optimitzar l'accés als serveis que actualment ofereix l'Agència, facilitant una gestió més eficient i basada en dades. Es concep com un element clau i innovador per a l'evolució contínua dels serveis de l'Agència, ja que permetrà incorporar noves funcionalitats i tecnologies, garantir el compliment normatiu vigent i afrontar amb garanties els reptes futurs en matèria de ciberseguretat.

1.3.2 Mòduls funcionals a desenvolupar en el marc del present contracte

El present contracte té per objecte la contractació del servei de disseny, implementació i posada en funcionament dels tres mòduls funcionals integrats a la Plataforma de governança de la ciberseguretat als àmbits, descrits a l'apartat anterior:

- Mòdul d'Operació
- Mòdul d'Avaluació
- Mòdul d'Adequació Normativa.

Aquests mòduls donaran cobertura a les diferents fases de la gestió de la ciberseguretat: des de la monitorització i explotació operativa, fins a l'avaluació del grau de compliment normatiu i la preparació documental per a processos d'auditoria i certificació, especialment en relació amb l'Esquema Nacional de Seguretat (ENS).

Els mòduls s'hauran d'integrar plenament, tant funcionalment com visualment, amb el Portal de Seguretat, que actua com a punt d'entrada unificat als serveis digitals de l'Agència. Aquesta integració ha de garantir una experiència d'usuari coherent, accessible i adaptada als diferents perfils d'usuari.

A més, cadascun dels mòduls haurà de generar i subministrar les mètriques i indicadors per construir el QCIC, el qual actuarà com a quadre de comandament central per a la governança de la ciberseguretat basada en dades. El QCIC oferirà una visió objectiva, consolidada i en temps real sobre l'estat de la ciberseguretat a tot el territori d'actuació de l'Agència, permetent una presa de decisions estratègica, informada i coordinada. Aquesta eina serà clau per al seguiment del progrés i l'avaluació de l'impacte de les accions impulsades, i esdevindrà un element fonamental per consolidar un model de governança orientat a resultats, compartit, eficient i capaç d'adaptar-se de manera contínua als reptes emergents del context digital.

El desenvolupament del QCIC correspon a l'adjudicatari del Mòdul d'Operació (Lot 1), que serà responsable de la seva implementació tècnica i desplegament. Tanmateix, els mòduls funcionals d'Avaluació (Lot 2) i Adequació Normativa (Lot 3) hauran de garantir la generació i compartició de les mètriques i els indicadors rellevants que permetin construir un quadre de comandament central, d'acord amb els requeriments funcionals definits per l'Agència.

1.4 Entorn tecnològic existent

L'Agència disposa d'un entorn tecnològic basat en serveis al núvol i solucions de l'ecosistema Microsoft, que donen suport a la gestió de dades, l'automatització de processos, el desplegament d'aplicacions i la incorporació de tecnologies d'intel·ligència artificial. Aquest entorn garanteix una base robusta, escalable i segura per al desenvolupament dels serveis digitals de l'Agència, així com per a la seva evolució futura.

Les principals solucions disponibles es poden agrupar en els àmbits següents::

- Infraestructura i gestió de dades
    - Microsoft Azure: plataforma de serveis al núvol que proporciona recursos d'infraestructura com màquines virtuals, emmagatzematge, bases de dades i serveis de xarxa, amb capacitat d'escalabilitat i gestió centralitzada.
    - Microsoft 365 E5: model de llicenciament que dona accés a aplicacions de productivitat (com Word, Excel, Teams), eines de col·laboració, serveis de ciberseguretat avançada i gestió de la informació.
    - SharePoint Online: aplicació inclosa a Microsoft 365 per a la gestió documental i com a repositori central de la base de coneixement corporativa. Permet l'organització, compartició i control d'accés als continguts de manera estructurada.
    - Microsoft Fabric: plataforma de dades que integra serveis per a la ingesta, transformació, governança i consulta de dades procedents de diverses fonts, facilitant-ne l'anàlisi unificada i en temps real.
    - Azure AI Search: servei de cerca i indexació basat en IA que permet recuperar informació rellevant a partir de documents estructurats i no estructurats mitjançant tècniques de processament del llenguatge natural i anàlisi semàntica.
- IA i automatització
    - Microsoft Copilot Studio: entorn de desenvolupament per a la creació d'assistents conversacionals mitjançant una interfície gràfica, amb suport per a publicació en múltiples canals (web, aplicacions de missatgeria o d'altre tipologia) i integració amb serveis externs.

  - Power Automate: plataforma per a la creació de fluxos de treball automatitzats entre aplicacions i serveis, amb capacitat per integrar sistemes interns i serveis de tercers mitjançant connectors predefinits o personalitzats.
  - Azure OpenAI: servei que dona accés a models d'IA generativa, com GPT-4o, a través d'API, amb capacitat per generar respostes i continguts a partir de diferents tipus d'entrada (documents de text o imatges) segons el model multimodal utilitzat.
- Anàlisi i visualització
  - Power BI: plataforma d'anàlisi de dades que permet crear informes i quadres de comandament interactius, útils per monitoritzar l'activitat dels assistents, identificar consultes recurrents i avaluar el rendiment i la qualitat de les respostes.

2 Lot 1: Mòdul d'Operació

2.1 Objecte i abast del servei

El present Lot té per objecte el disseny, desenvolupament i posada en funcionament d'una infraestructura central per al tractament de dades operatives de ciberseguretat. Aquesta ha de cobrir totes les fases del cicle de vida de la dada: des de la ingesta inicial, passant per la seva transformació i estructuració, fins a la seva explotació. El sistema haurà de garantir que les dades siguin consistents, traçables, segures i fàcilment reutilitzables, i posar-les a disposició mitjançant canals d'accés eficients com APIs, connectors, quadres de comandament i eines de visualització.

L'element central de la infraestructura serà una base de dades centralitzada amb capacitat per integrar fonts de dades diverses i heterogènies (amb dades estructurades o semiestructurades), incorporar funcionalitats de tractament automatitzat, escalar a volums *big data* i facilitar la integració de tecnologies d'intel·ligència artificial (tant per a l'entrenament de models propis com per a l'ús de serveis d'IA generativa). Aquesta base de dades haurà d'incorporar i absorbir les bases de dades actuals de l'Agència, garantint-ne la continuïtat operativa i la integració funcional.

A més, el present Lot inclou el disseny i desplegament del Quadre de Comandament Integral de Ciberseguretat (QCIC), que haurà d'oferir una visió consolidada, objectiva i en temps real de l'estat de la ciberseguretat als àmbits d'actuació de l'Agència. El QCIC actuarà com a eina estratègica per a la presa de decisions basada en dades i rebrà mètriques i indicadors operatius dels diferents mòduls de la plataforma.

El Mòdul d'Operació s'haurà de desplegar sota criteris d'escalabilitat, interoperabilitat i seguretat, i haurà de garantir una integració plena amb l'arquitectura tecnològica existent i amb la resta de components previstos en aquest Plec.

2.2 Objectius del servei

- Disposar d'una plataforma robusta, escalable i segura que permeti gestionar de manera eficient i centralitzada les dades massives (*big data*) operatives generades per l'activitat de l'Agència.
- Consolidar les dades operatives de l'Agència en un repositori únic que garanteixi la qualitat, protecció, disponibilitat i traçabilitat de les dades.
- Implementar un sistema d'informació de gestió completa del cicle de vida de les dades, incloent la ingesta des de múltiples fonts, la transformació i estructuració segons models definits, i la seva explotació.
- Desenvolupar mecanismes d'accés i explotació normalitzats, com ara API, connectors i quadres de comandament, que permetin consultar i analitzar la informació de manera eficient per a la presa de decisions.
- Desplegar una solució de governança de dades que permeti generar i administrar diccionaris, glossaris i metadades, així com definir i gestionar polítiques de qualitat i control d'accessos.
- Establir les bases tècniques i directrius comunes de governança de dades comunes per als desenvolupaments dels altres dos mòduls, garantint la coherència arquitectònica, semàntica i funcional de tota la plataforma en un sistema integrat.
- Desenvolupar i posar en funcionament el QCIC, integrant mètriques i indicadors dels tres mòduls, per oferir una visió unificada i centralitzada de l'estat de la ciberseguretat.
- Assegurar la integració, interoperabilitat i estil del mòdul amb la resta d'elements de la Plataforma de suport a la governança de la ciberseguretat.

2.3 Antecedents

L'Agència disposa de dues bases de dades principals en funcionament: la base de dades de l'Àrea d'operacions (InfoSOC) i la base de dades del servei de Govern de la dada (GDD). L'objectiu és que la nova base centralitzada integri i substitueixi amb funcionalitats actualitzades l'InfoSOC i la GDD.

Ambdues bases de dades es descriuen a continuació.

- InfoSOC

  Plataforma de referència per a la gestió, entre d'altres, d'actius, atacs rebuts, atacs gestionats, vulnerabilitats i mètriques d'activitat del SOC (Security Operations Center) de l'Agència. Dona suport a l'operativa de ciberseguretat i orquestració basada en dades.

  - Arquitectura general
    - Base de dades: MariaDB 10.3, més de 300 taules.
    - Infraestructura: desplegada en entorn *cloud* (Azure).
    - *Frontend*: accessible via web amb autenticació corporativa.
    - *Backend*: Django (Python), servidor d'aplicacions amb lògica de negoci, APIs REST.
    - Interfícies de visualització d'indicadors en quadres de comandament (PowerBI).
  - Dades origen
    - Inventaris i dades d'inventari obtingudes de la GDD.
    - Informació d'usuaris des de GICAR.
    - Vulnerabilitats escanejades des d'eines pròpies com Burp, Nessus, Acunetix o similars.
    - Vulnerabilitats de fonts des de fonts per subscripció de tercers com Shodan, Bitsight o amb funcionalitats de recollida de troballes de seguretat similars.
    - Registre d'identificadors públics (CVE) i detalls tècnics sobre vulnerabilitats crítiques des de fonts obertes de tercers.
    - Casos, peticions, incidents i tiquets operatius des de l'eina de tiqueting OTRS i d'automatització XSOAR.
    - Dades d'activitat, atacs rebuts i alertes des del SIEM de Splunk.
    - Dades introduïdes manualment des del *frontend*.
    - Informació sobre IPs, ports oberts, serveis actius, topologia de xarxa des de fitxers temporals de càrrega puntual subministrades per les entitats dels àmbits.
    - Correccions i dades contextuals específiques, introduïdes manualment pels tècnics o analistes des dels seus entorns de treball.
  - Base de dades i estructura interna
    - BBDD única (MariaDB) amb 300+ taules.
    - Model de dades estructurat per domini funcional: inventari, serveis, vulnerabilitats, usuaris o altres mètriques.
  - Automatització
    - Scripts de càrrega i processament (Python).
    - Automatització distribuïda amb cron en múltiples scripts *bash*.

        - Els diferents scripts gestionen funcions concretes (actualitzacions, càrrega, validació i altres accions automàtiques).
        - Execucions diàries, mensuals o puntuals segons el cas.
    - Accés i visualització
        - Interfície web amb funcionalitats de cerca, gestió d'actius, exportació i navegació entre entitats.
        - Vista de mètriques a través de quadres de comandament (PowerBI).
        - Accés a través de portal intern autenticat.
        - Consulta via API REST per a consum extern.

- GDD

  Servei centralitzat d'integració de dades de l'activitat de les diferents àrees i serveis de l'Agència. Ingesta, unifica, transforma i valida dades per a la seva explotació per altres sistemes o visualització.
    - Arquitectura general
        - Base de dades: Microsoft SQL Server, estructurada en 5 bases diferenciades.
        - Infraestructura: entorn *on-premise*, amb separació d'entorns de desenvolupament i producció.
        - *Frontend*: visualització a través de quadres de comandament (Power BI).
        - *Backend*: Processos ETL desenvolupats amb SSIS (SQL Server Integration Services) i consultes T-SQL.
        - Interfícies de visualització d'indicadors en quadres de comandament (PowerBI).
    - Dades origen
        - Inventaris, serveis, aplicacions i sistemes d'informació, des de fitxers estructurats (CSV o Excel).
        - Indicadors, registres operatius i dades de gestió, des de connexions directes a bases de dades o fitxers estructurats (CSV o Excel).
        - Informació d'anàlisi de vulnerabilitats sobre aplicacions, serveis i actius tecnològics des de l'API d'InfoSOC.
        - Correccions i dades contextuals específiques, introduïdes manualment pels tècnics o analistes des dels seus entorns de treball.
    - Base de dades i estructura interna
        - Base de dades Microsoft SQL Server, amb estructura segmentada en 5 blocs diferenciats.
        - Dades estructurades per domini funcional: serveis, aplicacions, usuaris, organitzacions, indicadors, catàlegs i configuració.
    - Automatització
        - Execució automatitzada mitjançant SQL Server Agent, amb calendaris de càrrega diària, setmanal o mensual segons el cas.
        - Automatització centralitzada, gestionada des del servidor de producció, amb paràmetres configurables.
        - Supervisió i registre de processos amb traçabilitat per data, procés, volum i estat d'execució.

- Interfícies externes i integració
  - Quadres de comandament a Power BI, accessibles via portal autenticat (https://app.powerbi.com), amb workspaces per servei i àrea.
  - Consulta estructurada sobre el *datawarehouse* mitjançant connectors.
  - Exportació de dades disponible a través de Power BI o extractes puntuals generats per l'equip funcional.

2.4 Activitats del servei

2.4.1 Disseny funcional

- Identificació, recollida i anàlisi dels requisits funcionals associats al Mòdul d'Operació, en coordinació amb l'equip de l'Agència.
- Disseny dels processos d'ingesta, transformació i explotació de dades, així com dels fluxos d'interacció entre el mòdul i altres components de la Plataforma de suport a la governança.
- Especificació dels casos d'ús, escenaris operatius i requeriments d'accés a la informació.
- Identificació de criteris d'acceptació per a cada funcionalitat clau.

2.4.2 Disseny de l'arquitectura i model de dades

- Disseny de l'arquitectura tècnica del sistema, tenint en compte l'escalabilitat, ciberseguretat i interoperabilitat amb l'ecosistema tecnològic de l'Agència.
- Identificació de les tecnologies de suport (bases de dades, plataformes de processament, sistemes de ciberseguretat i autenticació) i justificació de la seva selecció en funció dels requeriments no funcionals.
- Disseny detallat dels models de dades, incloent l'estructura de les taules, les relacions entre entitats, l'ús de claus primàries i estrangeres, les normalitzacions necessàries, i la definició dels camps clau per a garantir la qualitat, coherència i eficiència en la consulta i explotació de la informació.
- Establiment de mecanismes de control d'accés, monitorització, traçabilitat i gestió del cicle de vida de la informació.
- Integració amb canals d'explotació com APIs, connectors i eines de visualització.
- Definició de l'estratègia d'escalabilitat i continuïtat, incloent propostes d'arquitectura tolerants a fallades i amb alta disponibilitat.
- Adaptació de l'arquitectura per a la integració de solucions d'IA, tant per a l'entrenament de models propis com per a l'ús de serveis d'IA generativa externs.

2.4.3 Desenvolupament del Mòdul d'Operació

- Implementació dels components lògics i tècnics d'acord amb el disseny funcional, l'arquitectura i el model de dades dissenyats.
- Implementació de processos d'ingesta automatitzada de dades i de transformació segons els fluxos de dades definits.
- Implementació de funcionalitats per a la consulta, accés i explotació de la informació per part dels serveis interns.
- Implementació del QCIC a partir dels indicadors subministrats pels altres desenvolupaments definits en el present Plec.

2.4.4 Coordinació amb els mòduls en desenvolupament

- Coordinació i alineació funcional i tècnica amb els equips responsables dels altres desenvolupaments definits el present Plec, amb l'objectiu d'assegurar la coherència global de la Plataforma de suport a la governança.
- Intercanvi de mostres de dades, definició conjunta d'esquemes d'interoperabilitat i acord sobre formats, estructures semàntiques, taxonomies i mecanismes de sincronització de la informació.
- Participació activa en reunions tècniques de seguiment conjunt amb els responsables dels altres desenvolupaments definits el present Plec i del Portal de Seguretat, per garantir una integració fluida i el correcte encaix de les funcionalitats entre mòduls.

2.4.5 Proves i validació

- Elaboració del pla de proves del sistema, incloent proves unitàries, funcionals, d'integració i de rendiment.
- Execució de les proves previstes i documentació dels resultats obtinguts.
- Identificació i correcció d'incidències detectades durant la fase de validació.

2.4.6 Documentació i formació

- Redacció de la documentació tècnica i funcional dels diferents elements del mòdul (disseny d'arquitectura, manual d'ús, model de dades i configuració).
- Elaboració de guies d'ús i formació pràctica orientades al funcionament i administració del mòdul per part dels perfils operatius i tècnics de l'Agència.
- Transferència estructurada del coneixement per garantir la gestió i evolució futura del sistema per part dels equips interns.

2.5 Productes del servei

L'adjudicatari haurà de realitzar diverses activitats corresponents a les diferents fases del projecte per assegurar que els productes desenvolupats compleixen amb els requeriments establerts.

Per facilitar la comprensió del desplegament progressiu del projecte, es presenten a continuació terminis orientatius associats a les principals activitats. Aquests terminis tenen caràcter d'acord amb els objectius i requisits del contracte.

Activitat	Terminis màxims
Elaboració del disseny funcional	1 mes des de la formalització del contracte
Desenvolupament: MVP	3 mesos des de la formalització del contracte
Desenvolupament: final	8 mesos des de la formalització del contracte

2.5.1 Disseny funcional

2.5.1.1 Base de dades centralitzada d'operació de l'Agència

La base de dades centralitzada és l'element central del Mòdul d'Operació i ha de permetre consolidar, organitzar i explotar de manera eficient la informació operativa de l'Agència. Ha d'incorporar i actualitzar les funcionalitats que actualment desenvolupen l'InfoSOC i la GDD, ja que haurà de reemplaçar-les. El seu disseny ha d'estar estructurat de forma modular i escalable, amb un model de dades organitzat en blocs específics per àrea funcional. La base de dades haurà d'incloure canals d'accés diversos per a la ingesta i explotació de les dades (APIs, formularis, frontal web i quadres de comandament).

- Model de dades

  La nova base de dades que haurà de dissenyar i desenvolupar l'adjudicatari es divideix en un mínim de 10 models funcionals principals, cadascun centrat en una tipologia de dades específica i orientat a les funcions operatives de l'Agència.

  A continuació, es descriuen cadascun d'aquests models destacant les seves característiques principals.

  1. Model de taules mestres

     Centralitza les taules amb les dades estructurals que requereixen els diferents models del Mòdul d'Operació o poden requerir altres sistemes externs amb l'objectiu de garantir la coherència semàntica i tècnica de l'entorn tecnològic de l'Agència.

     Tipologia de dades:

     - Entitats del sector públic de la Generalitat de Catalunya i dels àmbits d'actuació de l'Agència.
     - Jerarquies institucionals.
     - Catàlegs de paràmetres de configuració, categoritzacions, tipologies o estats.

     Fonts principals:

     - InfoSOC i GDD (càrrega inicial).
     - Altres fonts de tercers de referència de tipus institucionals o serveis per subscripció.

  2. Model d'inventari

     Centralitza la informació sobre els actius tecnològics i organitzatius que formen part de l'ecosistema supervisat.

     Tipologia de dades:

     - Organitzacions, persones i rols.
     - Sistemes d'informació, aplicacions i versions.
     - Serveis, URLs, dominis.
     - Dispositius: servidors, portàtils, mòbils, impressores.
     - Adreces IP, ports i rangs de xarxa.
     - Entorns (producció, preproducció, proves).
     - Relacions entre actius: persona-dispositiu, sistema-servei o servei-IP.

     Fonts principals:

     - GDD i InfoSOC (càrrega inicial).
     - GICAR.
     - Bases de dades de proveïdors TI.
     - Bases de dades i fitxers d'inventaris subministrats per les entitats dels àmbits.

  3. Model d'orquestració

     Centralitza i vertebra l'intercanvi de dades entre els diferents models interns i amb plataformes d'automatització, permet definir les estratègies d'intercanvi amb altres models (incremental, periodicitat i horaris), actuant com a nucli operatiu per coordinar processos i accions automatitzades.

     Tipologia de dades:

- Instruccions, notificacions i missatges generats per les accions automatitzades.
- Registres d'execució de processos (estat, durada, resultats, volum processat).
- Històric d'interaccions entre models interns i fluxos automatitzats.

Fonts principals:

- Motor d'orquestració XSOAR de l'Agència (Palo Alto).
- Sistemes d'automatització d'aplicacions, tant internes com externes a l'Agència.

4. Model de perímetre

   Centralitza la informació que permet gestionar la validació i classificació del perímetre de seguretat aplicable a persones, sistemes i edificis.

   Tipologia de dades:

   - Catàleg de controls de ciberseguretat per nivell (base, avançat, complet).
   - Funcionalitats avaluades i evidències.
   - Resultats de revisió i valoració de grau de compliment.
   - Subjectes afectats (inventari d'actius i entitats).

   Fonts principals:

   - GDD i InfoSOC (càrrega inicial).
   - Eines d'operació de ciberseguretat de l'Agència.
   - SIEM de l'Agència (Splunk).
   - Bases de dades i fitxers d'inventaris subministrats per les entitats dels àmbits.

5. Model d'amenaces

   Centralitza el registre de les amenaces, la seva avaluació i el risc que evolucionin cap a incidents de ciberseguretat.

   Tipologia de dades:

   - Amenaces detectades (descripció, origen, categoria).
   - Classificació de l'amenaça i nivell de risc.
   - Fonts d'origen (intel·ligència externa o interna).
   - Relació amb vulnerabilitats, activitat gestionada, inventari d'actius i entitats.
   - Històric d'evolució.

   Fonts principals:

   - *Feeds* d'intel·ligència d'amenaces (*Threat Intel*) externs.
   - Bases de dades d'analítica d'amenaces internes de l'Agència (BBDD ElasticSearch de l'Àrea d'Operacions).

6. Model de vulnerabilitats

   Centralitza les vulnerabilitats tècniques detectades a l'ecosistema tecnològic supervisat.

   Tipologia de dades:

   - Identificadors CVE, puntuació de risc, descripció tècnica.
   - Vulnerabilitats detectades en IP/port o URL.
   - Relació amb inventari d'actius, entitats i amenaces.

- Estat de resolució o seguiment.
- Històric d'evolució.

Fonts principals:

- CVE.org
- Escaneigs tècnics d'eines pròpies: Nessus, Burp, Acunetix o similars.
- Fonts externes per subscripció: Bitsight, Shodan, Censys o similars.
- Bases de dades i fitxers de càrrega de la mà d'analistes o proveïdors externs.

7. Model d'activitat rebuda

   Centralitza el registre estructurat dels atacs reals rebuts sobre sistemes i serveis supervisats.

   Tipologia de dades:

   - Tipus d'atac, mètode, severitat, orígens.
   - Sistemes o dispositius afectats.
   - Relació amb inventari d'actius i entitats.
   - Històric d'evolució.

   Fonts principals:

   - SIEM de l'Agència (Splunk).
   - XSOAR de l'Agència (Palo Alto).

8. Model d'activitat gestionada

   Centralitza la gestió de les peticions, notificacions i incidències registrades pels sistemes de suport a l'operació.

   Tipologia de dades:

   - Casos gestionats: tipus, estat, dates, descripcions.
   - Informants (creadors del cas) i gestors tècnics.
   - Relació amb inventari d'actius i entitats.

   Fonts principals:

   - Eina de *tiqueting* OTRS de l'Agència.
   - XSOAR de l'Agència (Palo Alto).

9. Model d'avaluació

   Centralitza les dades generades pel Mòdul d'Avaluació (Lot 2) relatives a l'anàlisi del grau de compliment dels marcs normatius de ciberseguretat aplicables i els plans d'acció corresponents.

   Tipologia de dades:

   - Qüestionaris d'avaluació i respostes.
   - Indicadors de compliment normatiu, exposició davant amenaces i alineament amb el perímetre.
   - Plans d'acció derivats, amb accions recomanades i estat d'implementació.
   - Relació amb inventari d'actius i entitats.
   - Històric d'evolució.

Fonts principals:

- Mòdul d'Avaluació (Lot 2).

10. Model d'adequació normativa

Centralitza les dades generades pel Mòdul d'Adequació Normativa relatives al procés de preparació per a la certificació en l'ENS a partir d'evidències documentals.

Tipologia de dades:

- Evidències documentals.
- Controls normatius associats i grau d'adequació.
- Indicadors de validació de les evidències.
- Històric d'evolució.

Fonts principals:

- Mòdul d'Adequació Normativa (Lot 3).

- Consulta/extracció de dades

La nova base de dades haurà de disposar de diversos canals de consulta que permetin tant la interacció automatitzada entre sistemes com l'accés directe per part d'usuaris funcionals i tècnics. Aquests canals hauran de garantir la interoperabilitat, la seguretat d'accés i la disponibilitat de la informació en formats adequats per a la seva explotació.

  - API REST

    Proporcionarà un punt d'accés per a la consulta de dades entre el Mòdul d'Operació i altres aplicacions, tant interns (p. ex. el Portal de Seguretat) com externs a l'Agència (p. ex. la Plataforma Transversal de Dades de la Generalitat de Catalunya). L'API ha de garantir la integració operativa de la base de dades amb altres sistemes d'informació.

    Les funcionalitats principals són:

    - Subministrament centralitzat de taules mestre amb dades estructurals per garantir la coherència i unicitat del conjunt de sistemes de l'Agència.
    - Subministrament de dades d'inventari actualitzades.
    - Exportació en formats estructurats diversos (JSON, CSV).
    - Integració amb elements d'orquestració i automatització de processos.
    - Incorporació de control d'accés amb autenticació i autorització per rols (token OAuth2).

  - Frontal web

    Oferirà una interfície web accessible via navegador per a la consulta de dades. Estarà dissenyada per facilitar que els usuaris interns de l'Agència disposin accés a les dades i puguin realitzar operacions puntuals de visualització o extracció de dades.

    Les funcionalitats principals són:

    - Navegació entre les taules de diversos models de dades (p. ex. inventari d'actius, casos o vulnerabilitats).
    - Cerca avançada i filtració per atributs.
    - Informació de l'origen de les dades per, en cas d'identificar errors, poder identificar on realitzar correccions.
    - Exportació manual a Excel o CSV.

- Control d'accés mitjançant autenticació corporativa.

- Formularis web

  La nova base de dades permetrà capturar informació de formularis incrustats al web del Portal de Seguretat. Així, els usuaris autoritzats de les entitats dels àmbits podran introduir dades que s'ingestaran i emmagatzemaran de forma automàtica a la base de dades. Aquests mecanisme de captura de dades suposarà un mecanisme escalable per a la recollida de dades estructurades directament dels usuaris de les entitats dels àmbits d'actuació de l'Agència.

  Les funcionalitats principals són:

  - Recollida de les dades bàsiques de les entitats dels àmbits: nom, àmbit, responsables, dades de contacte i relacions.
  - Recollida de les dades dels actius TI de les entitats dels àmbits: sistemes, dispositius, serveis i IPs.
  - Recollida de respostes de qüestionaris.
  - Validació de la qualitat i consistència de les dades introduïdes als formularis per sol·licitar la seva revisió durant la ingesta a temps real.

2.5.1.2 Quadre de Comandament Integral de Ciberseguretat (QCIC)

El QCIC ha de permetre la visualització de mètriques i indicadors de ciberseguretat als àmbits d'actuació de l'Agència per donar suport a la presa de decisions tècniques i estratègiques.

El QCIC es construirà a partir dels quadres de comandament existents actualment a l'Agència, els quals permeten la visualització dels indicadors de l'InfoSOC i la GDD. Ara bé, a més, caldrà incorporar-hi els indicadors rellevants que subministraran els Mòduls d'Avaluació i Adequació Normativa, els quals estaran dissenyats per generar i compartir, de manera automàtica i periòdica, indicadors clau sobre el grau de compliment normatiu, l'estat de les autoavaluacions, la maduresa de la documentació aportada, les evidències disponibles i els plans d'acció definits. Aquestes dades hauran de ser emmagatzemades de manera estructurada a la base de dades centralitzada del Mòdul d'Operació, on podran ser consultats, agregats i representats visualment dins del QCIC. En conjunt,, aquesta integració garantirà una visió global i coherent de la ciberseguretat, facilitant una anàlisi transversal i una governança basada en dades.

Per tal que la visualització de dades sigui clara, estructurada i alineada amb les necessitats de governança, el disseny del QCIC ha de seguir criteris metodològics sòlids, inspirats en estàndards reconeguts de ciberseguretat i gestió del risc. L'objectiu és garantir que la informació es presenti de forma ordenada, jeràrquica i intel·ligible, afavorint tant la comprensió com la presa de decisions per part dels diferents perfils d'usuari. Aquests criteris han de permetre construir visualitzacions que expliquin una narrativa coherent (*storytelling with data*), facilitant la interpretació contextualitzada dels indicadors.

Com a referències per a l'enfocament conceptual, es proposa utilitzar un model com, per exemple, el de les tres línies de defensa del marc COSO (Committee of Sponsoring Organizations of the Treadway Commission), o bé el Cybersecurity Framework del NIST (National Institute of Standards and Technology), tots dos àmpliament adoptats i reconeguts per articular una governança eficaç basada en riscos i controls.

Les funcionalitats principals són:

- Integració completa amb el web del Portal de Seguretat com a interfície des d'on els usuaris accediran a les visualitzacions del QCIC.
- Compliment de criteris d'accessibilitat i usabilitat, amb disseny *responsive* i experiència d'usuari optimitzada.
- Capacitat per aplicar filtres dinàmics i multidimensionals: per entitat, data, territori, tipologia o estat de compliment,.

- Adaptació de visualitzacions segons perfil d'usuari: gestors globals, gestors d'àmbit i personal tècnic de cada entitat.
- Accés restringit de mètriques i indicadors de cada entitat només per als usuaris de les pròpies entitats.
- Exportació d'indicadors i informes en diversos formats (PDF, CSV, Excel) per facilitar la seva reutilització.
- Automatització de la generació d'informes i l'enviament per correu electrònic al usuaris de les entitats.

2.5.2 Disseny de l'arquitectura

Per garantir un funcionament robust i escalable, el Mòdul d'Operació haurà de basar-se en una arquitectura tècnica moderna i modular, capaç de gestionar grans volums de dades (*big data*), integrar múltiples fonts d'informació i facilitar la seva explotació. A més, el sistema haurà d'assegurar una interoperabilitat fluida amb els altres mòduls de la Plataforma de suport a la governança de la ciberseguretat.

- Tecnologia
  - El sistema es basarà en una arquitectura de dades de tipus medalló, organitzada en tres capes:
    - *Bronze*: ingesta de dades en brut i emmagatzematge sense transformar.
    - *Silver*: neteja, normalització i transformació de dades.
    - *Gold*: dades consolidades i optimitzades per a l'explotació i la generació d'indicadors.
  - La infraestructura haurà de suportar processos de tractament massiu de dades i actualitzacions recurrents, tot assegurant criteris estrictes de seguretat, disponibilitat, traçabilitat, governança i auditories d'accés.
  - La plataforma tecnològica utilitzada haurà de permetre:
    - Ingesta contínua i processament eficient de dades estructurades i no estructurades.
    - Definició i execució de fluxos ETL/ELT de manera integrada i escalable.
    - Gestió centralitzada del catàleg de dades i metadades.
    - Control d'accés per rols, qualitat de la dada, historial de modificacions i traçabilitat completa.
    - Integració nativa amb serveis de visualització i IA (com assistents, detecció d'anomalies o recomanacions).
  - Per al tractament de dades, es proposa l'ús de l'entorn d'Azure i Microsoft Fabric com a de base de dades *Big Data* al núvol, compatibles amb processos ETL, gestió escalable de dades i integració amb eines de governança.
  - Per a la visualització i explotació de dades, es proposa l'ús de Power BI, integrat dins del Portal de Seguretat, amb *dashboards* personalitzats per a cada perfil.
- Entrades i sortides del Mòdul (input/output)

Input	Output
- Dades d'InfoSOC i GDD (càrrega inicial). - Dades d'aplicacions internes. - Dades del sistema de fitxers intern.	- Dades d'indicadors consolidats per publicar a través del QCIC integrat en el Portal de Seguretat.

- Dades de fonts externes, tant obertes com de pagament. - Dades de formularis incrustats al Portal de Seguretat. - Dades del Mòdul d'Avaluació: qüestionaris, respostes i plans d'acció. - Dades del Mòdul d'Adequació Normativa: evidències i grau d'adequació.	- Dades i taules mestre per al funcionalment d'aplicacions internes i els mòduls definits al Plec a través de mecanisme ETL o API. - Dades per a aplicacions externes a través d'API. - Dades a través d'interfície web per a la consulta de personal tècnic intern.

- Integració amb la Plataforma de suport a la governança de la ciberseguretat dels àmbits

El Portal de Seguretat...	El Mòdul d'Avaluació (Lot 2)...	El Mòdul d'Adequació Normativa (Lot 3)...
- Proveeix l'accés autenticat als usuaris. - Permet visualitzar dades capturades directament de la base de dades centralitzada. - Publica els quadres de comandament del QCIC mitjançant components incrustables. - Disposa els formularis per ingestar directament les dades introduïdes pels usuaris.	- Captura dades (p. ex. entitats, vulnerabilitats, amenaces, proves tècniques i de *pentesting*) de la base de dades centralitzada per completar les dades dels qüestionaris. - Emmagatzema a la base de dades centralitzada les respostes dels qüestionaris i els plans d'acció. - Genera i comparteix els indicadors d'avaluació per mostrar al QCIC.	- Captura dades (p. ex. entitats, vulnerabilitats, amenaces i l'avaluació de les avaluacions) de la base de dades centralitzada per alimentar les evidències de l'ENS - Emmagatzema a la base de dades centralitzada l'avaluació de la validesa de les evidències. - Genera i comparteix els indicadors del grau de compliment de l'ENS per mostrar al QCIC.

2.5.3 Desenvolupament

L'adjudicatari haurà de lliurar una solució modular, dissenyada per complir amb el disseny funcional i ajustada al disseny d'arquitectura definit, amb l'objectiu de garantir una escalabilitat eficient i permetre l'evolució independent dels diferents components del sistema.

El desenvolupament s'haurà d'estructurar com a mínim en els següents blocs principals:

- La nova base de dades centralitzada
- El QCIC

La planificació del desenvolupament s'estructurarà, com a mínim, en els següents lliuraments:

- Producte Mínim Viable (MVP)
    - Lliurament d'una versió funcional inicial que permeti validar:
        - Configuració de la infraestructura.
        - 50% del model de dades de la base de dades.
        - ETL d'ingesta i emmagatzematge de les dades corresponents al model de dades desenvolupat.
        - Una API per a la consulta externa de dades.
        - Mostra d'un quadre de comandament del QCIC.

- Aquest MVP servirà com a base per a la realització d'iteracions successives i proves orientades a validar i millorar el funcionament del sistema.

- Lliurament final
  - Desenvolupament complet i estable del sistema, preparat per a la posada en producció.
  - Haurà d'incloure tots els mòduls descrits, integracions operatives i validació funcional completa.

2.5.4 Pla de proves i informe de resultats

El desenvolupament del servei seguirà una metodologia àgil i cada increment funcional lliurat haurà d'anar acompanyat del corresponent pla de proves i informe de resultats, amb l'objectiu de garantir la qualitat, la traçabilitat i el compliment dels requisits establerts.

- Pla de proves del sistema
  - Objectius generals i abast del pla de proves.
  - Metodologia i criteris d'acceptació.
  - Relació detallada dels tipus de proves:
    - Proves de *pipelines* (ingesta, processament i explotació): verificació del correcte funcionament dels fluxos de transformació i consolidació de dades.
    - Proves d'explotació de dades: accés mitjançant APIs, eines de visualització i exportació d'indicadors.
    - Proves de rendiment: resposta sota càrrega, escalabilitat i temps de procés.
    - Proves de ciberseguretat, control d'accés i registre d'activitat.
    - Proves d'integració amb altres sistemes: verificació del correcte intercanvi de dades i interoperabilitat amb el Portal i els desenvolupaments dels altres Lots.
    - Altres proves específiques segons les característiques de cada funcionalitat.
- Informe de resultats de les proves
  - Relació completa de proves executades amb el seu estat: superada / fallida / amb incidències.
  - Evidències tècniques: captures de pantalla, informes d'execució, registres de logs i mètriques.
  - Descripció de les incidències detectades i accions correctores aplicades o pendents.
  - Declaració de conformitat funcional del lliurament, que haurà de ser validada per l'Agència com a pas previ a la seva posada en producció.

2.5.5 Informe de ciberseguretat i compliment normatiu

Per tal de garantir que la solució desenvolupada compleix amb els requisits legals i tècnics exigibles, l'adjudicatari haurà d'elaborar i lliurar un informe conjunt que integri tant l'anàlisi de conformitat normativa com l'auditoria de ciberseguretat tècnica. Aquest document serà requisit indispensable per a l'acceptació del lliurament final i haurà de demostrar, de manera detallada, que el sistema desplegat és segur, resilient i alineat amb el marc regulador vigent.

- Informe de compliment de regulació

  Haurà d'avaluar, com a mínim, els següents marcs normatius:
  - Reglament General de Protecció de Dades (RGPD) i Llei Orgànica 3/2018, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD):
  - Esquema Nacional de Seguretat (ENS):

- Esquema Nacional d'Interoperabilitat (ENI), en la mesura que es prevegi l'intercanvi de dades o serveis amb altres sistemes públics.
- Altres regulacions que puguin ser d'aplicació.

- Informe d'auditoria de ciberseguretat

  Haurà d'avaluar, com a mínim, els aspectes següents:

  - Autenticació i control d'accés robust: identificació clara dels usuaris, aplicació del principi de privilegi mínim i segregació de funcions.
  - Protecció de la informació: xifratge de dades en repòs i en trànsit, integritat i disponibilitat dels actius d'informació.
  - Traçabilitat i registre d'activitats: registre d'esdeveniments rellevants, accés a dades i execució de processos.
  - Resiliència i continuïtat: proves d'estrès, capacitat de recuperació davant fallades, gestió de còpies de seguretat i disponibilitat.
  - Configuració segura i enduriment del sistema: actualització, eliminació de serveis innecessaris i protecció contra vulnerabilitats comunes.
  - Integració segura amb altres sistemes: validació dels mecanismes d'intercanvi de dades amb la resta de mòduls i serveis de l'Agència.
  - Anàlisi de vulnerabilitats i, si s'escau, proposta de mesures correctores.

2.5.6 Documents tècnics de tancament i sessions formatives

- Documentació tècnica
  - Disseny funcional.
  - Disseny de l'arquitectura.
  - Model de dades.
  - Diccionaris de dades, glossaris i metadades.
  - Documentació d'APIs i connectors: descripció funcional i tècnica dels serveis de compartició de dades, incloent especificacions, exemples de crida i paràmetres d'autenticació.
  - Manual d'administració del sistema global: operacions bàsiques de manteniment, gestió d'usuaris, configuració d'accessos, supervisió de processos, control de *logs* i seguiment del rendiment.
- Formació
  - Sessions tècniques per a administradors del sistema: enfocades en l'arquitectura, la configuració, la ciberseguretat, la monitorització i la gestió dels *pipelines* i integracions.
  - Model de suport post formació: proposta d'acompanyament inicial per part de l'adjudicatari, per garantir l'assimilació i autonomia progressiva dels equips interns.

2.6 Propostes de millora i evolució del servei

Amb l'objectiu d'augmentar el valor del servei i millorar-ne l'eficiència operativa, s'exposen diferents àrees on l'execució del contracte pot incloure aspectes de millora:

- Proposta de noves funcionalitats que amplïin les capacitats dels mòduls, millorin l'experiència d'ús o resolguin necessitats no cobertes en els requisits definits al Plec, sempre que estiguin alineades amb els objectius del servei.

- Propostes concretes per millorar el rendiment, optimitzar processos o enriquir la funcionalitat mitjançant tecnologies emergents com la intel·ligència artificial (IA), l'aprenentatge automàtic (ML), la RPA o solucions similars.
- Incorporació d'assistents virtuals (*xatbots*), motors de recomanació o altres eines que facilitin la interacció i l'ús dels mòduls.
- Propostes concretes d'integració amb els altres elements que conformen de la Plataforma de suport a la governança per millorar les funcionalitats, interoperabilitat o rendiment global.
- Integració amb fonts externes que aportin funcionalitats, context enriqueixin els resultats.
- Adopció de tècniques de millora contínua a partir de l'anàlisi del comportament del sistema, la detecció de patrons d'ús i el feedback dels usuaris.
- Possibilitat de configuració d'automatismes per a l'emissió d'alertes o la generació d'informes, de forma periòdica o basats en la detecció de desviacions o anomalies.

3 Lot 2: Mòdul d'Avaluació

3.1 Objecte i abast del servei

El present Lot té per objecte el disseny, implementació i desplegament d'un Mòdul d'Avaluació que permeti a les entitats dels àmbits d'actuació de l'Agència analitzar el seu nivell de ciberseguretat, tant pel que fa al grau d'exposició a les amenaces com al compliment dels principals marcs normatius. La solució haurà de permetre definir automàticament plans d'acció per millorar la postura de seguretat de cada entitat. El desplegament s'haurà de fer amb criteris d'escalabilitat, interoperabilitat i ciberseguretat, i integrar-se plenament amb l'arquitectura tecnològica existent de l'Agència i amb la resta de desenvolupaments descrits en aquest Plec.

Funcionalment, el Mòdul generarà qüestionaris adaptatius segons la naturalesa de cada entitat i el marc normatiu aplicable, estructurats per subdominis temàtics i en forma d'arbre lògic. El sistema haurà de centralitzar les respostes, automatitzar el càlcul d'indicadors de compliment i generar resultats contextualitzats, clars i accionables. Aquests resultats serviran per elaborar recomanacions específiques, definir plans d'acció personalitzats i fer seguiment de l'evolució del grau de compliment.

El Mòdul haurà de compartir mètriques i indicadors de maduresa en ciberseguretat amb el Quadre de Comandament Integral de Ciberseguretat (QCIC), de manera estructurada i estandarditzada, per alimentar el model de governança basada en dades de l'Agència.

3.2 Objectius del servei

- Fomentar l'autodiagnòstic i la cultura de la millora contínua en ciberseguretat dins les entitats, facilitant eines que promoguin l'autoresponsabilització, la transparència i el coneixement sobre el seu propi nivell de compliment.
- Millorar la capacitat de presa de decisions basada en dades, proporcionant a les entitats i a l'Agència una visió contextualitzada i objectiva de l'estat de la ciberseguretat, que serveixi de base per a la priorització d'inversions, accions correctores i estratègies de millora contínua.
- Proporcionar una eina escalable, robusta i interoperable per a l'avaluació del nivell de ciberseguretat de les entitats i el grau de compliment amb els principals marcs normatius, especialment l'Esquema Nacional de Seguretat (ENS).
- Generar qüestionaris d'avaluació, personalitzats, estructurats en forma d'arbre lògic i organitzats en subdominis temàtics, adaptats a la realitat, el nivell de maduresa i complexitat de cada entitat.
- Escalar la identificació de deficiències i oportunitats de millora a les entitats dels àmbits i automatitzar la definició de plans d'acció específics orientats a reforçar la postura de ciberseguretat de les entitats.
- Garantir l'automatització, escalabilitat i l'estandardització del procés d'avaluació i definició de plans d'acció, permetent aplicar-lo de manera eficient, coherent i homogènia a un gran volum d'entitats.
- Assegurar la integració del mòdul amb la resta d'elements de la Plataforma de suport a la governança de la ciberseguretat, incloent-hi el Portal de Seguretat i els mòduls desenvolupats en els altres lots del present plec.

3.3 Antecedents

L'Agència parteix d'un conjunt de formularis i procediments interns dissenyats per objectivar i normalitzar el desplegament dels serveis de ciberseguretat als diferents àmbits, prenent com a referència el grau de compliment de l'Esquema Nacional de Seguretat (ENS).

Aquest model d'avaluació es fonamenta en qüestionaris estructurats en forma d'arbre lògic, personalitzats per a cada entitat segons el marc de certificació aplicable dins l'ENS. En el cas del Perfil de Compliment Específic de Requisits Essencials de Seguretat (PCE-RES), el qüestionari consta de 127 preguntes organitzades en 11 subdominis. El Perfil de Compliment Específic per a l'àmbit de Salut (PCE-SALUD), per la seva banda, incorpora fins a 250 preguntes, incloent-hi les del PCE-RES i afegint-ne de noves específiques. Aquestes preguntes es distribueixen en àrees temàtiques com ara monitoratge del sistema, gestió del personal o protecció de serveis, entre d'altres.

El funcionament dels qüestionaris és adaptatiu: una resposta afirmativa pot activar preguntes dependents, mentre que una resposta negativa pot interrompre la branca corresponent, optimitzant així la càrrega de resposta i centrant l'anàlisi en els aspectes més rellevants per a cada entitat.

Tot i els avenços en estandardització i eficiència operativa aconseguits amb aquest model, el procés actual segueix requerint una elevada intervenció manual i no es recolza en una infraestructura tecnològica escalable ni automatitzada, la qual cosa limita la seva extensió a gran escala.

3.4 Activitats del servei

3.4.1 Disseny funcional

- Comprensió dels requisits funcionals associats al Mòdul d'Avaluació, en coordinació amb l'equip de l'Agència (no cal elaborar-lo des de zero, ja que l'Agència ja disposa del disseny funcional del desenvolupament).
- Modelatge lògic dels qüestionaris, definint l'estructura jeràrquica per subdominis temàtics i la lògica de navegació mitjançant arbres de decisions, adaptats al perfil, maduresa i complexitat de cada entitat, així com al marc normatiu aplicable.
- Definició de les regles de generació automàtica dels plans d'acció, així com del seu format, estructura de continguts i criteris de priorització, amb l'objectiu de garantir resultats clars, contextualitzats i accionables per a les entitats avaluades.
- Disseny de les dades que s'han de compartir amb el desenvolupament del Mòdul d'Operació i del Mòdul d'Adequació Normativa), així com dels indicadors a publicar al QCIC, definint-ne el format, la periodicitat i el mètode de transferència de dades, per garantir la coherència i interoperabilitat entre mòduls.

3.4.2 Disseny de l'arquitectura

- Disseny de l'arquitectura tècnica del sistema, garantint la modularitat, l'escalabilitat i la interoperabilitat amb l'ecosistema de l'Agència.
- Identificació de les tecnologies de suport (bases de dades, plataformes de processament, sistemes de ciberseguretat i autenticació) i justificació de la seva selecció en funció dels requeriments.
- Definició del model de dades que suportarà les respostes als qüestionaris, els resultats analítics i els plans d'acció generats.
- Definició de la integració de les dades amb la base de dades centralitzada i el QCIC desenvolupats pel Mòdul d'Operació.
- Definició de l'estratègia d'escalabilitat i continuïtat del servei, incloent propostes d'arquitectura tolerants a fallades i amb alta disponibilitat.

3.4.3 Desenvolupament del Mòdul d'Avaluació

- Implementació del sistema de gestió de perfils i rols d'usuari, amb control d'accés a funcionalitats i dades segons el perfil.

- Implementació del motor de qüestionaris adaptatius, configurable i compatible amb múltiples marcs normatius.
- Desenvolupament del motor generador d'informes personalitzats amb resultats, recomanacions i plans d'acció associats.
- Desenvolupament del sistema de càlcul automatitzat d'indicadors de compliment
- Desenvolupament de les interfícies web del sistema, dissenyades amb criteris d'usabilitat i accessibilitat, preparades per a la seva integració com a components incrustables dins del Portal de Seguretat.
- Desenvolupament dels mecanismes d'integració de les dades amb la base de dades centralitzada del Mòdul d'Operació, incloent-hi la preparació i l'exportació dels indicadors destinats al QCIC.

3.4.4 Coordinació amb els mòduls en desenvolupament

- Coordinació i alineació funcional i tècnica amb els equips responsables dels mòduls desenvolupats en els altres Lots, amb l'objectiu d'assegurar la coherència global de la plataforma.
- Intercanvi de mostres de dades, definició conjunta d'esquemes d'interoperabilitat i acord sobre formats, estructures semàntiques, taxonomies i mecanismes de sincronització de la informació.
- Participació activa en reunions tècniques de seguiment conjunt amb els responsables dels altres lots i del Portal de Seguretat, per garantir una integració fluida i el correcte encaix de les funcionalitats entre mòduls.
- Càrrega de les dades de forma persistent a la base de dades centralitzada del Mòdul d'Operació, així les mètriques i indicadors generats que es visualitzaran al QCIC.

3.4.5 Proves i validació

- Elaboració del pla de proves del sistema, incloent proves unitàries, funcionals, d'integració i de rendiment.
- Execució de les proves previstes i documentació dels resultats obtinguts.
- Identificació i correcció d'incidències detectades durant la fase de validació.

3.4.6 Documentació i formació

- Redacció de la documentació tècnica i funcional dels diferents elements del mòdul (disseny funcional, disseny de l'arquitectura, manual d'ús, manual d'administració i configuració).
- Elaboració de guies d'ús i formació pràctica orientades al funcionament i administració del mòdul per part dels perfils operatius i tècnics de l'Agència.
- Transferència estructurada del coneixement per garantir la gestió i evolució futura del sistema per part dels equips interns.

3.5 Productes del servei

L'adjudicatari haurà de realitzar diverses activitats corresponents a les diferents fases del projecte per assegurar que els productes desenvolupats compleixen amb els requeriments establerts.

Per facilitar la comprensió del desplegament progressiu del projecte, es presenten a continuació terminis orientatius associats a les principals activitats. Aquests terminis tenen caràcter d'acord amb els objectius i requisits del contracte.

Activitat	Terminis màxims
Elaboració del disseny funcional	1 mes des de la formalització del contracte
Desenvolupament: MVP	3 mesos des de la formalització del contracte

Desenvolupament: final	8 mesos des de la formalització del contracte

3.5.1 Disseny funcional

El Mòdul d'Avaluació ha de permetre que les entitats dels àmbits d'actuació de l'Agència puguin autoavaluar de manera automatitzada el seu grau d'exposició a l'amenaça cibernètica i el nivell de compliment normatiu. D'aquesta manera, la solució ha d'oferir, de forma automatitzada, informes contextualitzats, propostes de millora i plans d'acció, integrats amb el Portal de Seguretat i la resta de mòduls definits en aquest Plec.

L'Agència ja disposa del disseny funcional detallat del Mòdul d'Avaluació. Per tant, l'adjudicatari haurà de centrar-se en la seva comprensió, validació i, si escau, revisió o actualització, garantint-ne l'adequació funcional i tècnica.

Així, segons aquest disseny funcional, el desenvolupament ha de permetre la generació automàtica de qüestionaris particularitzats, per a cada entitat, amb l'objectiu avaluar el grau de compliment dels diferents marcs normatius. A partir de les respostes del qüestionari i de la incorporació de dades proves tècniques que mesuren el grau d'exposició a l'amenaça cibernètica, el desenvolupament ha de generar automàticament informes amb la diagnosi i els plans d'acció alineats amb els criteris de desplegament del perímetre de ciberseguretat definit per l'Agència.

En tot el desenvolupament, la solució ha de contemplar els mecanismes relacionats amb el govern de la dada com assegurar la qualitat de la informació, les metadades, gestionar els perfils i control d'accessos i la traçabilitat.

El sistema gestiona els estats progressius del procés d'avaluació: definició, assignació, execució, diagnosis, pla d'acció, tancament. Així, el procés funcional s'estructura en les següents fases:

1) Definició

En aquesta fase també es completa el formulari inicial de caracterització, que serveix com a base per configurar els qüestionaris d'avaluació personalitzats, adaptats a la realitat i necessitats de l'entitat.

Es dona d'alta l'entitat al sistema i se'n defineixen les característiques rellevants: àmbit d'actuació, tipus d'organització, maduresa en ciberseguretat, i altres atributs estructurals. A partir d'aquesta informació, es determina automàticament quins marcs normatius i de seguretat li són aplicables, així com el nivell d'exigència corresponent (ex. bàsic, mitjà, alt), i les amenaces cibernètiques principals que li apliquen.

2) Assignació

A partir de la informació recopilada en el formulari inicial, el sistema genera automàticament el qüestionari d'avaluació personalitzat, ajustat als marcs normatius aplicables, al nivell d'exigència i a les amenaces identificades per a l'entitat.

En aquesta fase també es defineix la planificació inicial de l'avaluació i s'assignen els consultors o responsables que duran a terme el procés. Aquesta assignació es fa amb la participació activa tant del personal de l'Agència com de l'entitat avaluada, garantint una visió compartida de l'abast i del calendari d'avaluació.

3) Execució

En aquesta fase es duu a terme la recopilació de la informació necessària per realitzar l'avaluació. Les dades s'obtenen a partir de fonts diverses, que inclouen:

- Les respostes proporcionades per l'entitat al qüestionari a través de formularis interactius incrustats al Portal de Seguretat.
- La informació disponible sobre el grau de compliment normatiu i configuració tècnica integrada automàticament des de la base de dades centralitzada del Mòdul d'Operació.

- Els resultats de proves tècniques, com exercicis de *pentesting* o simulacions d'atacs, també integrats automàticament des de la base de dades centralitzada del Mòdul d'Operació.

Aquest conjunt d'informació ha de permetre una avaluació objectiva, basada en qüestionaris i proves tècniques i orientada a la generació automàtica dels resultats posteriors.

4) Diagnosi

En aquesta fase, el sistema ha de revisar i avaluar totes les respostes recollides, així com la informació tècnica i de configuració obtinguda, per determinar el grau de compliment dels marcs de seguretat aplicables i el nivell d'exposició a les amenaces d'acord amb el perímetre de ciberseguretat establert per l'Agència.

Com a resultat, es genera l'Informe de Diagnosi que ha d'incloure els resultats detallats i ha de ser accessible des del Portal de Seguretat, dins de l'espai privat de cada entitat. Addicionalment, s'actualitzen els indicadors corresponents de l'entitat publicats al QCIC.

5) Acció

A partir dels resultats de la diagnosi, es revisen les necessitats detectades i es defineixen automàticament les iniciatives més adients per millorar la postura de ciberseguretat de l'entitat. Aquestes accions han de basar-se en un catàleg predefinit, estar prioritzades segons criteris objectius, i estar mapejades amb els marcs normatius corresponents.

6) Tancament

El sistema ha de generar de manera automatitzada l'Informe del Pla d'Acció, i ha de ser accessible des del Portal de Seguretat, dins de l'espai privat de cada entitat. Addicionalment, s'actualitzen els indicadors corresponents de l'entitat publicats al QCIC.

Per donar resposta a aquestes fases, el sistema haurà d'incloure les següents funcionalitats:

a) Gestió i configuració d'entitats

El sistema ha de permetre crear, definir i mantenir actualitzades les dades bàsiques de les entitats avaluades, així com la seva relació amb els marcs normatius aplicables. Inclourà:

- Creació i edició d'inventaris i característiques de les entitats dels àmbits d'actuació de l'Agència.
  - En general, les entitats seran creades per personal de l'Agència, tot i que existirà la possibilitat que l'entitat es doni d'alta ella mateixa inicialment, però el personal de l'Agència haurà de completar i validar el registre.
  - L'alta de l'entitat inclourà l'emplenament d'un qüestionari inicial per introduir informació com les dades generals, dades de contacte, matriu d'escalat i l'assignació del formulari d'avaluació que li correspongui.
  - Els usuaris autoritzats de l'Agència han de poder cercar per nom, àmbit o estat, donar-les d'alta i modificar-les, crear sub-entitats vinculades i assignar-los formularis.
  - Tant les pròpies entitats com el personal autoritzat de l'Agència podran realitzar modificacions i correccions a les dades de l'entitat.

L'element principal que formen part del model és:

- Formulari inicial configurable, amb preguntes a respondre agrupades per domini i subdomini que estaran habilitats en funció del tipus de pregunta i de les respostes anteriors. Els formularis s'han de poder cercar, donar-los d'alta, modificar-los, saber el percentatge de respostes completades i exportar-los a document Excel.

b) Gestió dels marcs (*frameworks*) per a l'avaluació

La gestió dels marcs de seguretat inclou la parametrització de les normes de seguretat a avaluar, les preguntes d'avaluació relacionades amb els controls, els criteris d'avaluació de les respostes dels qüestionaris i proves tècniques, i finalment els plans d'acció que se'n derivin.

Els elements principals que formen part del model són:

- Marcs normatius de seguretat: conjunt de principis bàsics, regulacions, requisits i mesures de ciberseguretat àmpliament utilitzats.
  - Els marcs normatius de seguretat poden provenir de normatives estàndard, o bé estar elaborats a mida per part de l'Agència.
  - S'han de poder crear, modificar i agrupar controls, també segmentar-los i crear fills, amb la finalitat d'acabar obtenint "controls-requeriments" (unitats elementals d'avaluació) que disposaran de la descripció corresponent.
  - El marcs de seguretat tindran versions en funció de la seva validesa (en definició, actives, obsoletes) i disposaran de diferents nivells de segmentació, però en tot cas caldrà poder avaluar un control-requeriment que pugui estar associat a un requeriment o el mateix requeriment. En aquest sentit, tots els requeriments han d'estar associats a, com a mínim, un control.
  - Els marcs de seguretat inclouran els esquemes de compliment de l'ENS (PCE-RES i PCE-SALUD, ampliables a altres com PCE-RIS) i d'altres com la normativa ISO 27001, ISO 27002, ISO 22301, NIS2 o RGPD. Es preveu un mapatge normatiu detallat per identificar l'alineament amb múltiples esquemes, per control i per bloc de preguntes.
- Marcs d'avaluació: agrupen les preguntes dels qüestionaris, les respostes, les proves tècniques i els mecanismes d'avaluació que permeten valorar el grau de compliment dels controls establerts.
  - Incorpora cadascuna de les preguntes relacionades amb un o més d'un control-requeriment i, al mateix temps, cada requeriment ha d'estar associats a, com a mínim, un control.
  - Els qüestionaris s'han de poder cercar, crear i editar, així com poder ser assignats a consultors / auditors que es donaran d'alta a l'aplicació.
  - Incorpora les respostes al formulari del tipus Sí/No i permet afegir un text opcional que permeti donar més detall.
  - Incorpora resultats de proves tècniques per complementar l'autoavaluació declarativa de les entitats amb evidències objectives i verificables sobre l'estat real dels sistemes (p. ex. resultats d'escaneigs de vulnerabilitats, exercicis de *pentesting* o anàlisis de configuracions) que permeten identificar debilitats concretes en la infraestructura i determinar de manera l'exposició a amenaces i el nivell efectiu de compliment.
  - Els mecanismes d'avaluació hauran d'admetre gestió de versions segons el seu cicle de vida (conceptualització, aplicació, obsolescència), i podran incorporar fórmules específiques de càlcul segons el tipus de pregunta (binària, ponderada o tècnica).
- Marcs d'accions de mitigació: catàleg d'iniciatives a realitzar per a cada control-requeriment que requereixi una acció de millora.
  - Les iniciatives són les que es duran a terme a partir de les respostes als formularis dels marcs d'avaluació. Cada acció disposarà de la seva descripció, objectius, abast, aplicabilitat, prioritat i estratègia de desplegament.

- Les accions han d'estar alineades amb les entitats i la seva definició, àmbit, tipus i diferents dades generals obtingudes a partir del formulari inicial de definició d'entitats.

c) Gestió de l'execució

Aquest bloc constitueix el nucli funcional del Mòdul d'Avaluació, ja que permet executar tot el procés d'avaluació automatitzada de les entitats. El model de dades relaciona les entitats, els marcs de control i les proves tècniques aplicables, els mecanismes d'avaluació i les accions de mitigació. Així, permet realitzar el mapeig entre les dades per obtenir diagnosis i plans d'acció en base a la parametrització inicial, les respostes als qüestionaris i els resultats de proves tècniques.

Les funcionalitats del bloc d'execució han d'incloure:

- Gestionar i executar el qüestionari inicial, definir els qüestionaris adaptatius i recollir les respostes.
- Crear i administrar els criteris d'avaluació, i els seus marcs corresponents, a aplicar a cada entitat.
- Aplicar els mecanismes d'avaluació i generar els resultats.
- Planificar les iniciatives de millora en funció de les respostes obtingudes i assignar automàticament les accions al consultor corresponent.
- Mantenir un històric complet de les modificacions de respostes, càlculs i accions. Per controlar el cicle de vida de l'avaluació.
- Definir diferents usuaris autoritzats segons el rol (gestor, consultor i tècnic de l'entitat), els quals hauran de disposar dels privilegis d'edició i consulta corresponents.

Els elements principals que formen part del model són:

- Respostes: conté l'arbre de respostes recollides durant l'avaluació, incloent mecanismes d'avaluació, càlculs numèrics i no numèrics, exposició a vulnerabilitats, evidències tècniques, i assignació d'iniciatives.
- Vulnerabilitats: associades a cada avaluació, contindran informació detallada sobre cada vulnerabilitat detectada en proes tècniques, com la descripció, CVE, actius afectats, eines d'identificació i evolució.
- Avaluació: entitat principal que recull tota la informació relacionada amb el procés d'avaluació, com la descripció, entitat objecte, estat, responsables, període d'execució, *frameworks* aplicats, consultors assignats, resultats, informes finals i valoracions.
- Iniciatives: actuacions proposades automàticament en funció de les respostes i resultats, vinculades als controls avaluats i orientades a millorar la postura de ciberseguretat.

d) Generació automàtica d'indicadors

Es vol automatitzar el càlcul i visualització d'un conjunt d'indicadors per cada fase del procés que permeti realitzar la gestió i el seguiment de l'avaluació del compliment dels marcs de ciberseguretat i s'integri amb al QCIC publicat a través del Portal de Seguretat.

- Indicadors: aquests indicadors i llistats necessaris per analitzar els resultats de les avaluacions realitzades inclouran aspectes relacionats amb:
  - Càlcul del compliment.
  - Exposició davant possibles amenaces.
  - Alineament amb el perímetre.
  - Iniciatives dels plans d'acció.
  - Grau d'execució de les iniciatives.

e) Generació automàtica d'informes

La solució ha de ser capaç de generar automàticament un Informe de Diagnosi i Plans d'acció que es lliuraran a l'entitat després de l'avaluació.

- L'informe d'avaluació: proporciona una avaluació sobre l'exposició a les principals amenaces i l'estat de compliment normatiu. Destaca els punts forts i punts febles i proporciona una visió operativa i estratègica, incloent inversions i estratègies, en funció de la criticitat dels sistemes exposats i altres variables.
- El pla d'acció: detalla les accions i mesures correctores proposades per abordar les deficiències detectades. Aquestes accions hauran d'estar mapejades amb els controls normatius corresponents i prioritzades segons el grau de risc.
- Cada informe disposarà d'una versió executiva.

Aquests informes han d'estar subjectes a uns processos de validació ni la gestió documental i quedar accessibles dins del portal de seguretat, en l'espai privat de cada entitat.

f) Assistent conversacional

Es vol disposar d'un agent conversacional incrustat al Portal de Seguretat capaç de donar suport als usuaris. Podrà interpretar i respondre dubtes en diversos idiomes i donar resposta. L'agent ha de ser capaç de resoldre dubtes que puguin tenir els usuaris de les entitats respecte a:

- Com avançar en el procés, indicant les passes i la informació a preparar.
- Com omplir els qüestionaris, resolent dubtes sobre terminologia i normativa a través d'exemples.
- Altres tasques de suport que puguin suposar una ajuda per a l'usuari.

3.5.2 Disseny de l'arquitectura

La solució haurà de basar-se en una arquitectura modular, interoperable i flexible, preparada per adaptar-se a diferents marcs normatius i a un elevat volum d'entitats. El sistema ha d'incloure capacitats de gestió centralitzada de qüestionaris, avaluació automatitzada, generació de plans d'acció i càlcul d'indicadors, tot garantint la integració amb el Portal de Seguretat i la resta de desenvolupaments descrits en el present Plec.

- Tecnologia
  - Arquitectura de microserveis que permeti una millor escalabilitat, mantenibilitat i evolució independent dels components.
  - Contenidors Docker, per facilitar el desplegament, la portabilitat i la gestió dels entorns.
  - Motor de qüestionaris configurable, amb lògica condicional, agrupació temàtica i flexibilitat per adaptar-se a diferents normatives.
  - Base de dades estructurada per gestionar preguntes, respostes, puntuacions, plans d'acció i perfils d'usuari.
  - Capa de connectivitat o API REST per compartir dades amb el Mòdul d'Operacions, el Mòdul d'Adequació Normativa i el Portal de Seguretat.
  - Persistència de dades al repositori centralitzat del Mòdul d'Operacions, assegurant la traçabilitat i la coherència de la informació.
  - Integració amb una interfície *web responsive* per als perfils d'entitats, gestors i supervisió.

- Entrades i sortides del Mòdul (input/output):

Input	Output
- Dades contextuals de les entitats, introduïdes pel personal autoritzat de l'Agència: tipologia, mida i grau de maduresa. - Dades del Mòdul d'Operació: perímetre, amenaces i proves tècniques. - Qüestionaris d'avaluació que apliquen a cada entitat generats pel personal autoritzat de l'Agència. - Dades de formularis incrustats al Portal de Seguretat amb les respostes proporcionades per les entitats avaluades. - Regles lògiques per avaluar el grau de compliment definides pel personal autoritzat de l'Agència. - Feedback o actualitzacions d'estat per part de les entitats o gestors ingestades a través del Portal de Seguretat.	- Informe de diagnosi accessible des del Portal de Seguretat. - Informe de pla d'acció accessible des del Portal de Seguretat. - Dades de les respostes al qüestionari, avaluació, plans d'acció i evolució de la seva execució per emmagatzemar l'històric en el Mòdul d'Operació. - Dades d'indicadors consolidats per al Mòdul d'Operació per publicar a través del QCIC al Portal de Seguretat.

- Integració amb la Plataforma de suport a la governança de la ciberseguretat dels àmbits

El Portal de Seguretat...	El Mòdul d'Operació (Lot 1)...	El Mòdul d'Adequació Normativa (Lot 3)...
- Proveeix l'accés autenticat als usuaris. - Disposa els formularis incrustats per ingestar directament les respostes als qüestionaris introduïdes per les entitats. - Publica els informes generats - Publica els indicadors dels quadres de comandament del QCIC mitjançant elements incrustables.	- Comparteix dades (p. ex. entitats, vulnerabilitats, amenaces i proves tècniques) per completar la informació dels qüestionaris. - Allotja l'històric de dades de les respostes dels qüestionaris i els plans d'acció. - Captura i publica els indicadors al QCIC.	- Captura les dades dels resultats de l'avaluació de compliment dels controls de l'ENS, ja que s'utilitzaran per preparar la captura d'evidències.

3.5.3 Desenvolupament

L'adjudicatari haurà de lliurar una solució modular, dissenyada per complir amb el disseny funcional i ajustada al disseny d'arquitectura definit, amb l'objectiu de garantir una escalabilitat eficient i permetre l'evolució independent dels diferents components del sistema.

La planificació del desenvolupament s'estructurarà, com a mínim, en els següents lliuraments:

- Producte Mínim Viable (MVP)
    - Lliurament d'una versió funcional inicial que permeti validar:

        - Configuració de la infraestructura.
        - Interacció bàsica amb l'usuari d'una entitat.
        - Generació i gestió d'un qüestionari adaptatiu a partir d'un formulari inicial.
        - Producció d'un esborrany d'informe d'avaluació de compliment.
        - Càlcul preliminar d'indicadors a publicar al QCIC.
    - Aquest MVP servirà com a base per a la realització d'iteracions successives i proves orientades a validar i millorar el funcionament del sistema.
- Lliurament final
    - Desenvolupament complet i estable del sistema, preparat per a la posada en producció.
    - Haurà d'incloure tots els mòduls descrits, integracions operatives i validació funcional completa.

3.5.4 Pla de proves i informe de resultats

El desenvolupament del servei seguirà una metodologia àgil i cada increment funcional lliurat haurà d'anar acompanyat del corresponent pla de proves i informe de resultats, amb l'objectiu de garantir la qualitat, la traçabilitat i el compliment dels requisits establerts.

- Pla de proves del sistema
    - Objectius generals i abast del pla de proves.
    - Metodologia i criteris d'acceptació.
    - Relació detallada dels tipus de proves:
        - Proves de creació i gestió de qüestionaris segons casos d'ús.
        - Proves de generació automatitzada d'informes.
        - Proves de la lògica de càlcul automatitzada, i la generació d'indicadors qualitatius i quantitatius a partir de les respostes.
        - Proves d'usabilitat, navegació i experiència d'usuari en l'ús de la interfície i els indicadors del QCIC a través del Portal de Seguretat.
        - Proves de ciberseguretat, control d'accés i registre d'activitat.
        - Proves d'integració amb altres sistemes: verificació del correcte intercanvi de dades i interoperabilitat amb el Portal i els desenvolupaments dels altres Lots.
        - Altres proves específiques segons les característiques de cada funcionalitat.
- Informe de resultats de les proves
    - Relació completa de proves executades amb el seu estat: superada / fallida / amb incidències.
    - Evidències tècniques: captures de pantalla, informes d'execució, registres de logs i mètriques.
    - Descripció de les incidències detectades i accions correctores aplicades o pendents.
    - Declaració de conformitat funcional del lliurament, que haurà de ser validada per l'Agència com a pas previ a la seva posada en producció.

3.5.5 Informe de ciberseguretat i compliment normatiu

Per tal de garantir que la solució desenvolupada compleix amb els requisits legals i tècnics exigibles, l'adjudicatari haurà d'elaborar i lliurar un informe conjunt que integri tant l'anàlisi de conformitat normativa com l'auditoria de ciberseguretat tècnica. Aquest document serà requisit indispensable per

a l'acceptació del lliurament final i haurà de demostrar, de manera detallada, que el sistema desplegat és segur, resilient i alineat amb el marc regulador vigent.

- Informe de compliment de regulació

  Haurà d'avaluar, com a mínim, els següents marcs normatius:

  - Reglament General de Protecció de Dades (RGPD) i Llei Orgànica 3/2018, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD):
  - Esquema Nacional de Seguretat (ENS):
  - Altres regulacions que puguin ser d'aplicació.

- Informe d'auditoria de ciberseguretat

  Haurà d'avaluar, com a mínim, els aspectes següents:

  - Autenticació i control d'accés robust: identificació clara dels usuaris, aplicació del principi de privilegi mínim i segregació de funcions.
  - Protecció de la informació: xifrat de dades en repòs i en trànsit, integritat i disponibilitat dels actius d'informació.
  - Traçabilitat i registre d'activitats: registre d'esdeveniments rellevants, accés a dades i execució de processos.
  - Resiliència i continuïtat: proves d'estrès, capacitat de recuperació davant fallades, gestió de còpies de seguretat i disponibilitat.
  - Configuració segura i enduriment del sistema: actualització, eliminació de serveis innecessaris i protecció contra vulnerabilitats comunes.
  - Integració segura amb altres sistemes: validació dels mecanismes d'intercanvi de dades amb la resta de mòduls i serveis de l'Agència.
  - Anàlisi de vulnerabilitats i, si s'escau, proposta de mesures correctores.

3.5.6 Documents tècnics de tancament i sessions formatives

- Documentació tècnica
  - Disseny funcional.
  - Disseny de l'arquitectura.
  - Model de dades.
  - Diccionaris de dades, glossaris i metadades.
  - Documentació d'APIs i connectors: descripció funcional i tècnica dels serveis de compartició de dades, incloent especificacions, exemples de crida i paràmetres d'autenticació.
  - Manual d'administració del sistema global: operacions bàsiques de manteniment, gestió d'usuaris, configuració d'accessos, supervisió de processos, control de *logs* i seguiment del rendiment.

- Formació
  - Sessions tècniques per als usuaris dels àmbits: enfocades a dotar de competències per a l'ús de l'eina.
  - Sessions tècniques per a administradors del sistema: enfocades en l'arquitectura, la configuració, la ciberseguretat, la monitorització i la gestió de les dades i integracions.
  - Model de suport postformació: proposta d'acompanyament inicial per part de l'adjudicatari, per garantir l'assimilació i autonomia progressiva dels equips interns.

3.6 Propostes de millora i evolució del servei

Amb l'objectiu d'augmentar el valor del servei i millorar-ne l'eficiència operativa, s'exposen diferents àrees on l'execució del contracte pot incloure aspectes de millora:

- Proposta de noves funcionalitats que amplïin les capacitats dels mòduls, millorin l'experiència d'ús o resolguin necessitats no cobertes en els requisits definits al Plec, sempre que estiguin alineades amb els objectius del servei.
- Propostes concretes per millorar el rendiment, optimitzar processos o enriquir la funcionalitat mitjançant tecnologies emergents com la intel·ligència artificial (IA), l'aprenentatge automàtic (ML), la RPA o solucions similars.
- Incorporació d'assistents virtuals (*xatbots*), motors de recomanació o altres eines que facilitin la interacció i l'ús dels mòduls.
- Propostes concretes d'integració amb els altres elements que conformen de la Plataforma de suport a la governança per millorar les funcionalitats, interoperabilitat o rendiment global.
- Integració amb fonts externes que aportin funcionalitats, context enriqueixin els resultats.
- Adopció de tècniques de millora contínua a partir de l'anàlisi del comportament del sistema, la detecció de patrons d'ús i el feedback dels usuaris.
- Possibilitat de configuració d'automatismes per a l'emissió d'alertes o la generació d'informes, de forma periòdica o basats en la detecció de desviacions o anomalies.

4 Lot 3: Mòdul d'Adequació Normativa

4.1 Objecte i abast del servei

El present Lot té per objecte el disseny, implementació i desplegament d'un Mòdul d'Adequació Normativa que permeti optimitzar les tasques prèvies a una auditoria de certificació en l'Esquema Nacional de Seguretat (ENS). Aquesta solució haurà de desplegar-se amb criteris d'escalabilitat, interoperabilitat i ciberseguretat, i s'haurà d'integrar plenament amb l'arquitectura tecnològica existent de l'Agència i amb la resta de desenvolupaments descrits en aquest Plec.

Funcionalment, el Mòdul haurà de facilitar la recollida ordenada i la gestió eficient de la documentació i les evidències que permetin acreditar el compliment dels requisits establerts per l'ENS. Mitjançant l'ús de tècniques d'intel·ligència artificial, la solució haurà de ser capaç de validar automàticament la qualitat, la rellevància i l'adequació de les evidències, així com d'avaluar el grau de preparació normativa de cada entitat de cara al procés de certificació. El sistema haurà de garantir la traçabilitat i la integritat de les evidències, i facilitar-ne l'extracció de manera conjunta per a la seva presentació en una posterior auditoria de certificació.

El Mòdul haurà de compartir mètriques i indicadors del nivell de preparació i les evidències disponibles per al compliment de l'ENS, amb el Quadre de Comandament Integral de Ciberseguretat (QCIC), de manera estructurada i estandarditzada, per alimentar el model de governança basada en dades de l'Agència.

4.2 Objectius del servei

- Fomentar l'autodiagnòstic i la preparació estructurada per a la certificació de l'ENS, proporcionant a les entitats eines que facilitin la recopilació, classificació i validació d'evidències documentals, amb l'objectiu de reforçar la seva capacitat d'autoresponsabilització cap al compliment dels requisits normatius de ciberseguretat.
- Proporcionar una eina escalable, automatitzada i eficient que doni suport al procés de recollida, classificació, validació i gestió de les evidències de compliment per a un gran volum d'entitats.
- Dissenyar una solució que optimitzi, simplifiqui i estandarditzi en el procés de recollida i validació de la qualitat, rellevància i idoneïtat de les evidències les evidències necessàries anterior a la sol·licitud d'una auditoria de certificació en l'ENS.
- Garantir la centralització, traçabilitat i reutilització en futurs processos de revisió o certificació de les evidències, reduint errors i augmentant la fiabilitat i eficiència del procés.
- Assegurar la integració del mòdul amb la resta d'elements de la Plataforma de suport a la governança de la ciberseguretat, incloent-hi el Portal de Seguretat i els mòduls desenvolupats en els altres lots del present plec.

4.3 Antecedents

L'Agència ha estat reconeguda com a Òrgan d'Auditoria Tècnica (OAT) pel Centro Criptológico Nacional (CCN) per poder realitzar auditories de conformitat amb l'ENS a l'Administració de la Generalitat de Catalunya i al seu sector públic, a les entitats locals i a aquelles altres entitats que estiguin sota l'àmbit competencial de l'Agència. L'Agència és responsable de donar suport i emetre el certificat de l'ENS a les entitats públiques catalanes, un total de més de 2000 entitats que compleixen amb els requisits de protecció i seguretat de la informació per a certificar-se.

Amb l'obtenció del certificat, les entintats poden acreditar formalment que compleixen amb el que estableix el Perfil de Compliment Específic de Requisits Essencials de Seguretat (PCE-RES) i el Perfil de Compliment Específic per a l'àmbit de Salut (PCE-SALUD), els quals inclouen mesures de

ciberseguretat, tant tecnològiques com organitzatives L'objectiu del PCE-RES i PCE-SALUD és protegir la informació i els serveis prestats, per això és necessari adoptar mesures de ciberseguretat, entre les quals s'inclouen normatives, configuració de sistemes, auditories, gestió d'incidents o programes de formació.

L'ENS proporciona un marc comú de principis bàsics, requisits mínims i mesures de ciberseguretat per protegir adequadament els serveis prestats i la informació tractada per les administracions públiques. Tant les administracions com els seus proveïdors han de demostrar el compliment amb l'ENS a través de declaracions o certificacions de conformitat.

Els processos d'auditories de certificació que l'OAT pot dur a terme poden ser de qualsevol de les categories que estableix l'ENS i dels Perfils de Compliment Específic (PCE) existents. Els certificats tenen una validesa de dos anys i, un cop superat aquest termini, és necessari tornar a certificar-se, ja sigui en el mateix perfil de compliment o categoria, o en un de superior, sempre que s'hagi realitzat l'adequació prèvia.

S'ofereixen dues modalitats d'auditoria:

1. Auditories d'adequació als diferents nivells de l'esquema que consisteixen en un conjunt de proves i de revisió documental de les evidències realitzades in-situ.
2. Auditories de compliment dels requisits essencials de ciberseguretat utilitzant principalment dues eines del CCN-CERT:
    - INES, la qual permet recollir informació i evidències de cada entitat de forma organitzada, delegada i supervisada al llarg de l'any.
    - AMPARO, la qual facilita els processos d'auditoria de conformitat i avalua la conformitat del sistema, facilitant la gestió de la certificació de conformitat.

4.4 Activitats del servei

4.4.1 Elaboració del disseny funcional

- Identificació, recollida i anàlisi dels requisits funcionals associats al Mòdul d'Avaluació, en coordinació amb l'equip de l'Agència.
- Disseny dels processos de recollida, gestió i classificació d'evidències, incloent els fluxos de validació, generació automatitzada de recomanacions i preparació estructurada per a l'auditoria de certificació.
- Establiment dels criteris i mecanismes per a la validació automatitzada d'evidències, mitjançant l'ús de tècniques d'intel·ligència artificial, amb l'objectiu de garantir-ne la qualitat, rellevància i adequació normativa.

4.4.2 Disseny de l'arquitectura

- Disseny de l'arquitectura tècnica del sistema, garantint la modularitat, l'escalabilitat i la interoperabilitat amb l'ecosistema de l'Agència.
- Identificació de les tecnologies de suport (bases de dades, plataformes de processament, sistemes de ciberseguretat i autenticació) i justificació de la seva selecció en funció dels requeriments no funcionals.
- Definició del model de dades que suportarà la recollida, emmagatzematge i anàlisi de les evidències.
- Definició de la integració de les dades amb la base de dades centralitzada i el QCIC desenvolupats pel Mòdul d'Operació.

- Definició de l'estratègia d'escalabilitat i continuïtat del servei, incloent propostes d'arquitectura tolerants a fallades i amb alta disponibilitat.

4.4.3 Desenvolupament del Mòdul d'Adequació Normativa

- Implementació del sistema de gestió de perfils i rols d'usuari, amb control d'accés a funcionalitats i dades segons el perfil.
- Implementació del sistema per a la captura, classificació i validació automatitzada d'evidències documentals vinculades als requisits de conformitat normativa.
- Desenvolupament de funcionalitats per a la gestió documental, orientades a facilitar la preparació estructurada i eficient de les entitats davant processos d'auditoria i certificació.
- Desenvolupament del *prompting* específic per a l'ús de sistemes d'intel·ligència artificial multimodal, amb capacitat per analitzar les evidències aportades, identificar-ne la validesa i generar comentaris contextualitzats i interpretables per l'usuari.
- Desenvolupament de les interfícies web del sistema, dissenyades amb criteris d'usabilitat i accessibilitat, preparades per a la seva integració com a components incrustables dins del Portal de Seguretat.
- Desenvolupament dels mecanismes d'integració de les dades amb la base de dades centralitzada del Mòdul d'Operació, incloent-hi la preparació i l'exportació dels indicadors destinats al QCIC.

4.4.4 Coordinació amb els mòduls en desenvolupament

- Coordinació i alineació funcional i tècnica amb els equips responsables dels mòduls desenvolupats en els altres lots, amb l'objectiu d'assegurar la coherència global de la plataforma.
- Intercanvi de mostres de dades, definició conjunta d'esquemes d'interoperabilitat i acord sobre formats, estructures semàntiques, taxonomies i mecanismes de sincronització de la informació.
- Participació activa en reunions tècniques de seguiment conjunt amb els responsables dels altres lots i del Portal de Seguretat, per garantir una integració fluida i el correcte encaix de les funcionalitats entre mòduls.
- Càrrega de les dades de forma persistent a la base de dades centralitzada del Mòdul d'Operació, així les mètriques i indicadors generats que es visualitzaran al QCIC.

4.4.5 Proves i validació

- Elaboració del pla de proves del sistema, incloent proves unitàries, funcionals, d'integració i de rendiment.
- Execució de les proves previstes i documentació dels resultats obtinguts.
- Identificació i correcció d'incidències detectades durant la fase de validació.

4.4.6 Documentació i formació

- Redacció de la documentació tècnica i funcional dels diferents elements del mòdul (disseny funcional, disseny de l'arquitectura, manual d'ús, manual d'administració i configuració).
- Elaboració de guies d'ús i formació pràctica orientades al funcionament i administració del mòdul per part dels perfils operatius i tècnics de l'Agència.
- Transferència estructurada del coneixement per garantir la gestió i evolució futura del sistema per part dels equips interns.

4.5 Productes del servei

L'adjudicatari haurà de realitzar diverses activitats corresponents a les diferents fases del projecte per assegurar que els productes desenvolupats compleixen amb els requeriments establerts.

Per facilitar la comprensió del desplegament progressiu del projecte, es presenten a continuació terminis orientatius associats a les principals activitats. Aquests terminis tenen caràcter d'acord amb els objectius i requisits del contracte.

Activitat	Terminis màxims
Elaboració del disseny funcional	1 mes des de la formalització del contracte
Desenvolupament: MVP	3 mesos des de la formalització del contracte
Desenvolupament: final	8 mesos des de la formalització del contracte

4.5.1 Disseny funcional

Es requereix desenvolupar, o integrar una eina comercial, que permeti definir l'estratègia de recollida i validació de les evidències, així com el seguiment de l'evolució del nivell de compliment dels controls de l'ENS per a cada entitat.

En tot el desenvolupament, la solució ha de contemplar els mecanismes relacionats amb el govern de la dada com assegurar la qualitat de la informació, les metadades, gestionar els perfils i control d'accessos i la traçabilitat.

Per tal d'assolir-ho, es requereix disposar dels següents blocs funcionals:

a) Gestió documental d'evidències

- Permetrà la captura i emmagatzematge, a través del Portal de Seguretat, de les evidències que serviran per validar el compliment dels controls de l'ENS.
- Sempre que sigui possible, les evidències s'hauran d'obtenir de manera automatitzada, a partir dels sistemes de l'entitat a avaluar o dels propis sistemes de l'Agència, per reduir la càrrega manual i millorar la fiabilitat de la informació.
- S'inclouran funcionalitats completes de gestió documental, que permetin el control de versions, el registre de canvis i la traçabilitat de cada evidència.
- El sistema haurà de contemplar l'assignació múltiple d'una evidència: quan una mateixa evidència sigui aplicable a més d'una entitat, s'ha de poder associar de forma directa i eficient a totes elles.

b) Avaluació automàtica preliminar de les evidències

- El sistema haurà d'incloure una funcionalitat d'anàlisi automatitzada que permeti realitzar una avaluació preliminar de la qualitat, validesa i coherència de les evidències aportades, mitjançant l'ús d'intel·ligència artificial.
- El sistema de validació de les evidències garantirà la seguretat i la confidencialitat de la informació gestionada. Podrà emprar-se el servei d'intel·ligència artificial generativa multimodal de la infraestructura Azure de l'Agència, mitjançant l'ús de la seva API.
- Aquesta anàlisi s'haurà de basar en un servei de *prompting* específicament dissenyat per interpretar les evidències en relació amb els requeriments, criteris d'acceptació i polítiques de certificació de l'Esquema Nacional de Seguretat (ENS).
- Addicionalment, el sistema haurà de permetre al personal autoritzat incorporar anotacions i comentaris sobre cada evidència, així com modificar manualment l'estat de validesa en cas que calgui complementar o corregir l'avaluació automàtica realitzada.
- El resultat de l'anàlisi constituirà una pre-auditoria automàtica que indiqui si les evidències presentades són suficients i adequades per donar compliment als controls requerits,

detectant mancances o desviacions que caldrà corregir abans d'iniciar un procés formal d'auditoria.

c) Extracció massiva d'evidències

- Un cop totes les evidències hagin estat validades, el sistema permetrà la descàrrega massiva de les evidències emmagatzemades a través del Portal de Seguretat per part dels usuaris degudament autoritzats.
- Sempre que sigui possible, s'automatitzarà el procés de preparació i càrrega d'aquestes evidències en format massiu i directe cap a la plataforma INES del CCN-CERT, d'acord amb els requeriments tècnics i procediments establerts per aquest organisme.

d) Monitorització contínua del compliment del marc de ciberseguretat

- Desenvolupament d'una eina transversal de monitorització contínua del compliment dels diferents marcs de ciberseguretat a través d'una recollida automatitzada d'evidències, i en concret, del compliment de l'ENS.
- Queda oberta la possibilitat d'utilitzar solucions existents ja siguin comercials o disponibles públicament, com seria el cas del conjunt d'eines d'anàlisi de logs, xifrat, *backup*, que ofereix el CCN-CERT.

e) Generació automàtica d'informes d'auditoria:

- El sistema haurà de generar automàticament una versió preliminar de l'informe d'auditoria tècnica a partir de les evidències aportades i validades, els controls aplicables i l'estat de compliment de cada requisit del marc ENS.
- Aquest informe haurà de seguir una estructura coherent amb els models i formats exigits pel CCN-CERT per a l'obtenció del certificat ENS i haurà d'incloure:
  - Una síntesi de les evidències per cada control i requeriment.
  - L'estat de conformitat (conforme/no conforme/parcial) de cada control.
  - Una valoració qualitativa de la solidesa de les evidències presentades.
  - Un llistat de mancances detectades, si escau, amb la seva gravetat i impacte estimat.
- La generació de l'informe s'haurà de basar en les dades emmagatzemades en el sistema i les anàlisis automàtiques prèvies, fent ús de tècniques d'IA generativa quan sigui convenient per elaborar textos preliminars, com justificacions, resums o recomanacions.
- El sistema també haurà de permetre la revisió i validació manual de l'informe per part del personal autoritzat de l'Agència.
- L'informe s'haurà de generar en format editable i en format final (PDF signable) i quedarà accessible per a cada entitat dins el seu espai privat al Portal de Seguretat.

f) Centralització de dades històriques i indicadors:

- Es transferiran de manera estructurada i segura les dades clau generades durant el procés d'adequació cap a la base de dades centralitzada del Mòdul d'Operació, amb l'objectiu de mantenir un històric complet i fiable per a la seva traçabilitat i reutilització.
- El sistema haurà de generar i posar a disposició els indicadors derivats del procés d'adequació normativa per a la seva visualització dins del QCIC, garantint que siguin estructurats, comparables i orientats a la presa de decisions estratègiques.

g) Supervisió del funcionament correcte de la plataforma:

- Es disposarà de proves de control automatitzades i recurrents per assegurar una supervisió contínua del correcte funcionament de la plataforma i notificacions immediates en cas d'errors o resultats inesperats.

g) Assistent conversacional

Es vol disposar d'un agent conversacional incrustat al Portal de Seguretat capaç de donar suport als usuaris. Podrà interpretar i respondre dubtes en diversos idiomes i donar resposta. L'agent ha de ser capaç de resoldre dubtes que puguin tenir els usuaris de les entitats respecte a:

- Com avançar en el procés, indicant les passes i la informació a preparar.
- Com carregar les evidències, resolent dubtes sobre terminologia a través d'exemples.
- Com aportar evidències vàlides.
- Altres tasques de suport que puguin suposar una ajuda per a l'usuari.

4.5.2 Disseny de l'arquitectura

El Mòdul d'Adequació Normativa s'ha de basar en una arquitectura flexible, segura i orientada a processos, capaç de gestionar la documentació prèvia a la certificació en el marc de ciberseguretat de l'ENS. Aquesta arquitectura ha de facilitar la recollida, classificació, validació i explotació d'evidències normatives, tot garantint la integració amb el Portal de Seguretat i la resta de desenvolupaments descrits en el present Plec.

- Tecnologia
  - Arquitectura de microserveis, que permet una millor escalabilitat, mantenibilitat i evolució independent dels components.
  - Contenidors Docker, per facilitar el desplegament, la portabilitat i la gestió dels entorns.
  - Repositori estructurat d'evidències amb etiquetatge, control de versions i validació d'adequació.
  - Motor documental per a la ingesta, tractament, indexació i gestió de les evidències documentals aportades per les entitats.
  - Ús d'un servei d'intel·ligència artificial multimodal per validar la qualitat, rellevància i cobertura normativa de les evidències aportades de diferent naturalesa, com documents de text o imatges.
  - Capa de connectivitat o API REST per compartir dades amb el Mòdul d'Operacions, el Mòdul d'Adequació Normativa i el Portal de Seguretat.
  - Integració amb una interfície web responsive per als perfils d'entitats per a càrrega assistida de documents i seguiment del progrés dels plans d'acció.
- Entrades i sortides del Mòdul (input/output):

Input	Output
- Dades del Mòdul d'Avaluació: llistats de requisits normatius per a cada entitat importats i estat del nivell de compliment informat. - Evidències documentals carregades per les entitats a través d'una interfície incrustada al Portal de Seguretat.	- Informe d'adequació normativa detallat sobre les evidències i grau de validesa. - Dades de la recollida i validació de les evidències per emmagatzemar l'històric en el Mòdul d'Operació - Dades d'indicadors consolidats per al Mòdul d'Operació per publicar a través del QCIC al Portal de Seguretat.

- Integració amb la Plataforma de suport a la governança de la ciberseguretat dels àmbits

El Portal de Seguretat...	El Mòdul d'Operació (Lot 1)...	El Mòdul d'Adequació Normativa (Lot 2)...
- Proveeix l'accés autenticat als usuaris. - Disposa de la interfície incrustada per a la càrrega de les evidències. - Disposa de la interfície de treball i gestió de les evidències pel personal autoritzat. - Publica els informes generats. - Publica els indicadors dels quadres de comandament del QCIC mitjançant elements incrustables.	- Allotja l'històric de dades de les evidències i validació. - Captura i publica els indicadors al QCIC.	- Comparateix les dades dels resultats de l'avaluació de compliment dels controls de l'ENS, ja que s'utilitzaran per preparar la captura d'evidències.

4.5.3 Desenvolupament

L'adjudicatari haurà de lliurar una solució modular orientada a facilitar la preparació de les entitats per a l'obtenció de certificacions en matèria de ciberseguretat, amb especial atenció al compliment de l'Esquema Nacional de Seguretat (ENS). El sistema ha d'incorporar funcionalitats per a la recollida estructurada d'evidències, la validació automatitzada mitjançant IA, la generació d'informes previs a auditoria i la integració amb altres sistemes de la plataforma de governança.

La planificació del desenvolupament s'estructurarà, com a mínim, en els següents lliuraments:

- Producte Mínim Viable (MVP)
    - Lliurament d'una versió funcional inicial que permeti validar:
        - Configuració de la infraestructura.
        - Interacció bàsica amb un usuari per a la càrrega d'evidències i seguiment del seu estat.
        - Classificació automàtica de documents.
        - Validació preliminar de les evidències d'una selecció de controls de l'ENS representatius mitjançant motor d'IA..
    - Aquest MVP servirà com a base per a la realització d'iteracions successives i proves orientades a validar i millorar el funcionament del sistema.
- Lliurament final
    - Desenvolupament complet i estable del sistema, preparat per a la posada en producció.
    - Haurà d'incloure tots els mòduls descrits, integracions operatives i validació funcional completa.

4.5.4 Pla de proves i informe de resultats

El desenvolupament del servei seguirà una metodologia àgil i cada increment funcional lliurat haurà d'anar acompanyat del corresponent pla de proves i informe de resultats, amb l'objectiu de garantir la qualitat, la traçabilitat i el compliment dels requisits establerts.

- Pla de proves del sistema
    - Objectius generals i abast del pla de proves.
    - Metodologia i criteris d'acceptació.
    - Relació detallada dels tipus de proves:
        - Proves de càrrega i validació d'evidències amb la ingesta massiva de documentació.
        - Proves de verificació del *prompting* per a la verificació de les evidències mitjançant IA generativa.
        - Proves de seguiment i traçabilitat per a una correcta gestió del cicle de vida de les evidències (versions, dates o validacions).
        - Proves de generació automatitzada d'informes.
        - Proves de la interacció del personal autoritzat de l'Agència per incorporar anotacions manuals i revisions de la validació de les evidències.
        - Proves de simulació de processos per d'exportació de paquets d'evidències per a l'auditoria de certificació.
        - Proves de generació d'informes.
        - Proves de ciberseguretat, control d'accés i registre d'activitat.
        - Proves d'integració amb altres sistemes: verificació del correcte intercanvi de dades i interoperabilitat amb el Portal i els desenvolupaments dels altres Lots.
        - Altres proves específiques segons les característiques de cada funcionalitat.
- Informe de resultats de les proves
    - Relació completa de proves executades amb el seu estat (superada / fallida / amb incidències).
    - Evidències tècniques: captures de pantalla, informes d'execució, registres de logs i mètriques.
    - Validació de la funcionalitat del sistema per gestionar, classificar i explotar evidències documentals.
    - Avaluació específica del comportament del sistema en la integració amb altres mòduls, amb identificació de problemes i solucions aplicades.
    - Informació quantitativa sobre temps de validació d'evidències, capacitat de càrrega i ús de recursos.
    - Descripció de les incidències detectades i accions correctores aplicades.
    - Valoració global respecte als criteris d'acceptació.
    - Recomanacions tècniques per a la millora del sistema, si escau.
    - Declaració de conformitat, validada per l'Agència, com a pas previ per a la posada en producció.
- Informe de compliment de regulació

  Haurà d'avaluar, com a mínim, els següents marcs normatius:
    - Reglament General de Protecció de Dades (RGPD) i Llei Orgànica 3/2018, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD):
    - Esquema Nacional de Seguretat (ENS):

- Esquema Nacional d'Interoperabilitat (ENI), en la mesura que es prevegi l'intercanvi de dades o serveis amb altres sistemes públics.
- Altres regulacions que puguin ser d'aplicació.

- Informe d'auditoria de ciberseguretat

  Haurà d'avaluar, com a mínim, els aspectes següents:

  - Autenticació i control d'accés robust: identificació clara dels usuaris, aplicació del principi de privilegi mínim i segregació de funcions.
  - Protecció de la informació: xifrat de dades en repòs i en trànsit, integritat i disponibilitat dels actius d'informació.
  - Traçabilitat i registre d'activitats: registre d'esdeveniments rellevants, accés a dades i execució de processos.
  - Resiliència i continuïtat: proves d'estrès, capacitat de recuperació davant fallades, gestió de còpies de ciberseguretat i disponibilitat.
  - Configuració segura i enduriment del sistema: actualització, eliminació de serveis innecessaris i protecció contra vulnerabilitats comunes (OWASP).
  - Integració segura amb altres sistemes: validació dels mecanismes d'intercanvi de dades amb la resta de mòduls i serveis de l'Agència.
  - Anàlisi de vulnerabilitats i, si s'escau, proposta de mesures correctores.

4.5.5 Documents tècnics de tancament i sessions formatives

- Documentació tècnica
  - Disseny funcional
  - Disseny de l'arquitectura
  - Manual d'ús per als usuaris dels àmbits: guia bàsica per a la utilització de l'eina.
  - Manual d'administració del sistema: operacions bàsiques de manteniment, gestió d'usuaris, configuració d'accessos, supervisió de processos, control de *logs* i seguiment del rendiment.
- Formació
  - Sessions tècniques per als usuaris dels àmbits: enfocades a dotar de competències per a l'ús de l'eina.
  - Sessions tècniques per a administradors del sistema: enfocades en l'arquitectura, la configuració, la ciberseguretat, la monitorització i la gestió de les dades i integracions.
  - Model de suport postformació: proposta d'acompanyament inicial per part de l'adjudicatari, per garantir l'assimilació i autonomia progressiva dels equips interns.

4.6 Propostes de millora i evolució del servei

Amb l'objectiu d'augmentar el valor del servei i millorar-ne l'eficiència operativa, s'exposen diferents àrees on l'execució del contracte pot incloure aspectes de millora:

- Proposta de noves funcionalitats que amplïin les capacitats dels mòduls, millorin l'experiència d'ús o resolguin necessitats no cobertes en els requisits definits al Plec, sempre que estiguin alineades amb els objectius del servei.
- Propostes concretes per millorar el rendiment, optimitzar processos o enriquir la funcionalitat mitjançant tecnologies emergents com la intel·ligència artificial (IA), l'aprenentatge automàtic (ML), la RPA o solucions similars.

- Incorporació d'assistents virtuals (*xatbots*), motors de recomanació o altres eines que facilitin la interacció i l'ús dels mòduls.
- Propostes concretes d'integració amb els altres elements que conformen de la Plataforma de suport a la governança per millorar les funcionalitats, interoperabilitat o rendiment global.
- Integració amb fonts externes que aportin funcionalitats, context enriqueixin els resultats.
- Adopció de tècniques de millora contínua a partir de l'anàlisi del comportament del sistema, la detecció de patrons d'ús i el feedback dels usuaris.
- Possibilitat de configuració d'automatismes per a l'emissió d'alertes o la generació d'informes, de forma periòdica o basats en la detecció de desviacions o anomalies.

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.

Els equips prestataris dels serveis estaran ubicats físicament a les oficines de l'adjudicatari, o bé en alguna altra que ambdues parts acordin, atenent sempre a la seguretat de la informació gestionada pel servei.

Tot i això, en cas que l'Agència ho requereixi, s'autoritzarà la prestació/execució de fins al 50% de les tasques/projectes/serveis amb recursos ubicats a les instal·lacions de l'Agència a l'Hospitalet de Llobregat i l'adjudicatari estarà obligat a ajustar-s'hi.

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 i perfils

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos de l'adjudicatari del contracte 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.

Es requereix un equip de treball de diferents perfils, amb dedicacions específiques, un pla de treball i organigrama conjunt, per a l'execució dels serveis sol·licitats en els apartats d'aquest plec.

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

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.

5.3.1 Lot 1: Mòdul d'Operació

- Equip de treball

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **5.929 hores**.

Dins del total d'hores establertes per a l'execució del contracte, l'adjudicatari haurà de garantir la disponibilitat dels perfils professionals necessaris per complir amb els requeriments del servei.

A títol orientatiu, la següent taula presenta una estimació dels perfils mínims i les responsabilitats principals requerides per al correcte desenvolupament del servei.

Perfil	Dedicació respecte del total del contracte	Responsabilitats principals
Project Manager	5%	Planificació, coordinació general del projecte, seguiment, interlocució amb l'Agència, control de qualitat i terminis…
Arquitecte de dades	10%	Disseny de l'arquitectura tècnica, model de dades i estratègia d'interoperabilitat entre mòduls i sistemes…
Enginyer de dades	60%	Desenvolupament de pipelines, ingestes, transformació, processos ETL, integració tècnica i ciberseguretat de les dades…
Científic de dades	5%	Definició i explotació d'indicadors per al QCIC, exploració i preparació de dades…
Consultor de visualitzacions de dades	10%	Desenvolupament del QCIC, visualitzacions, panells i exportació d'indicadors…
Consultor Especialista	10%	Disseny funcional, suport formatiu, elaboració de documentació, auditoria de ciberseguretat, eines de governança de la dada, innovació i assessorament estratègic…

- Perfils

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

Perfil	Requisit
Project Manager	5 anys d'experiència
Arquitecte de dades	3 anys d'experiència
Enginyer de dades	
Científic de dades	
Consultor de visualitzacions de dades	
Consultor Especialista	

L'Agència identifica aquests perfils com a necessaris per la prestació d'aquest servei, tot i que serà l'adjudicatari qui els haurà d'ajustar la composició de l'equip i la dedicació global dels mateixos per garantir desplegament.

5.3.2 Lot 2: Mòdul d'Avaluació

- Equip de treball

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **3.143 hores**.

Dins del total d'hores establertes per a l'execució del contracte, l'adjudicatari haurà de garantir la disponibilitat dels perfils professionals necessaris per complir amb els requeriments del servei.

A títol orientatiu, la següent taula presenta una estimació dels perfils mínims i les responsabilitats principals requerides per al correcte desenvolupament del servei.

Perfil	Dedicació respecte del total del contracte	Responsabilitats principals
Project Manager	5%	Planificació, coordinació general del projecte, seguiment, interlocució amb l'Agència, control de qualitat i terminis...
Arquitecte de dades	10%	Disseny de l'arquitectura tècnica, model de dades i estratègia d'interoperabilitat entre mòduls i sistemes...
Enginyer de dades	30%	Ingesta de fonts de dades i dels formularis dels usuaris, desenvolupament del motor de dades, integraciówde dades amb la BBDD centralitzada, desenvolupament de pipelines, desenvolupament d'indicadors del QCIC...
Tècnic / Desenvolupador	30%	Desenvolupament de la interfície per incrustar al web del Portal de Seguretat, desenvolupament de funcionalitats addicionals...
Científic de dades	5%	Supevisió de la qualitat de les dades, Disseny dels indicadors a visualitzar en el QCIC...
Consultor Especialista	20%	Disseny funcional, suport formatiu, elaboració de documentació, auditoria de ciberseguretat, eines de governança de la dada, innovació i assessorament estratègic...

- Perfils

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

Perfil	Requisit
Project Manager	5 anys d'experiència
Arquitecte de dades	3 anys d'experiència
Enginyer de dades	
Tècnic / Desenvolupador	
Científic de dades	
Consultor Especialista	

L'Agència identifica aquests perfils com a necessaris per la prestació d'aquest servei, tot i que serà l'adjudicatari qui els haurà d'ajustar la composició de l'equip i la dedicació global dels mateixos per garantir desplegament.

5.3.3 Lot 3: Mòdul d'Adequació Normativa

- Equip de treball

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **3.143 hores**.

Dins del total d'hores establertes per a l'execució del contracte, l'adjudicatari haurà de garantir la disponibilitat dels perfils professionals necessaris per complir amb els requeriments del servei.

A títol orientatiu, la següent taula presenta una estimació dels perfils mínims i les responsabilitats principals requerides per al correcte desenvolupament del servei.

Perfil	Dedicació respecte del total del contracte	Responsabilitats principals
Project Manager	5%	Planificació, coordinació general del projecte, seguiment, interlocució amb l'Agència, control de qualitat i terminis...
Arquitecte de dades	10%	Disseny de l'arquitectura tècnica, model de dades i estratègia d'interoperabilitat entre mòduls i sistemes...
Enginyer de dades	25%	Ingesta de fonts de dades i dels formularis dels usuaris, desenvolupament del motor de dades, integració de dades amb la BBDD centralitzada, desenvolupament de pipelines, desenvolupament d'indicadors del QCIC...
Tècnic / Desenvolupador	25%	Desenvolupament de la interfície web incrustable al Portal de Seguretat, integració de funcionalitats de gestió d'evidències per a usuaris i administradors...
Científic de dades	5%	Desenvolupament de prompting i configuració d'IA per a la validació d'evidències, supervisió de la qualitat de les dades, disseny dels indicadors a visualitzar en el QCIC...
Consultor Especialista	30%	Disseny funcional, suport formatiu, elaboració de documentació, auditoria de ciberseguretat, eines de governança de la dada, innovació i assessorament estratègic...

- Perfils

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

Perfil	Requisit
Project Manager	5 anys d'experiència
Arquitecte de dades	3 anys d'experiència
Enginyer de dades	
Tècnic / Desenvolupador	
Científic de dades	
Consultor Especialista	

L'Agència identifica aquests perfils com a necessaris per la prestació d'aquest servei, tot i que serà l'adjudicatari qui els haurà d'ajustar la composició de l'equip i la dedicació global dels mateixos per garantir desplegament.

5.4 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte 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. 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 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.

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 ciberseguretat 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 i, especialment, l'impuls de la transformació fonamentada en el coneixement col·laboratiu, la coordinació de l'ecosistema de ciberseguretat i la voluntat per la innovació continua, es requereix que l'empresa adjudicatària registri tot el coneixement que disposi i es generi en la contractació que derivi 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, 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 ciberseguretat 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, durant l'horari d'execució del servei, 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 ciberseguretat, 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 (especialment ENS, LOPDGDD, RGPD, LSSI).

A la finalització del contracte, l'adjudicatari quedarà obligat al lliurament o destrucció en cas de ser sol·licitada, de de la informació obtinguda o generada com a conseqüència de la prestació del servei en un termini màxim de 48 hores. Aquesta informació pot incloure el codi de programació desenvolupat o allotjat en entorns de desenvolupament de l'adjudicatari, o bé la documentació subministrada per l'Agència per facilitar l'execució del contracte.

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. L'Agència farà una notificació prèvia per a la realització de tasques d'auditoria, encara que no requereixin la col·laboració activa per part del personal de l'adjudicatari, 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 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.

5.11 Formació

El personal de l'empresa adjudicatària del contracte realitzarà formació continuada per tal de garantir l'actualització dels seus coneixements, així com l'adquisició de nous coneixements, que puguin ser de valor en els serveis requerits per l'Agència.

5.12 Contingència

Els adjudicataris hauran de proveir un pla de contingència, en cas de desastre de les instal·lacions principals, en unes instal·lacions alternatives (centre de gestió secundari) on l'adjudicatari pugui executar la seva activitat, que inclouran:

- Estacions de treball amb el programari adequat per realitzar les tasques descrites.
- Comunicacions d'accés a les aplicacions informàtiques.
- Telefonia fixa a les instal·lacions del servei.
- Accés a Internet a través de la xarxa d'àrea local.
- Espai suficient per allotjar en condicions de treball òptimes:
    - El personal necessari de l'adjudicatari per realitzar el servei i
    - Personal de l'Agència, o de terceres parts determinades per aquest, per a la correcta gestió del servei.
- Pla i execució de proves per validar la solució de contingència implementada, amb la periodicitat que l'Agència determini.

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

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.

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, 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 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 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 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 podrà requerir a l'empresa adjudicatària del contracte el lliurament de la documentació acreditativa de la conformitat amb l'ENS. L'empresa adjudicatària del contracte haurà de designar, segons estableix l'ENS, un punt de contacte per a la ciberseguretat (POC) que canalitzarà i supervisarà el compliment dels requisits de ciberseguretat 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 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. Especialment haurà de complir amb la Política de ciberseguretat 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 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 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 ha de garantir que tot el personal sigui conscienciat, rebi formació i informació sobre els seus deures, obligacions i responsabilitats en matèria de ciberseguretat derivats de la legislació, del marc normatiu intern i dels procediments i directrius aplicables, així com 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 ciberseguretat

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 i software), aquests hauran de ser compatibles amb l'arquitectura de ciberseguretat de l'Agència i complir amb els requeriments de ciberseguretat que estableixi el marc legal i el marc normatiu intern, sotmetre's a proves tècniques de ciberseguretat 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 des de la fase de disseny fins a la posada en producció.

L'empresa adjudicatària del contracte 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 ciberseguretat 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 ciberseguretat relacionada amb el seu objecte d'adquisició. Els productes o serveis de ciberseguretat hauran de constar al Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del Centre Criptològic Nacional (CCN) 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 CCN 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 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 haurà de garantir que es documentin com a mínim les característiques de la interfície, els requisits de ciberseguretat 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 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 ciberseguretat 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 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. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència de Ciberseguretat.

5.14.8 Incidents de ciberseguretat

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

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

5.14.9 Accés a la informació

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

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

Les empreses adjudicatària haurà de presentar un informe de seguiment de cada contracte 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, 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 contracte.

- Un informe de dedicació del contracte 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 contracte, 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 o el que es determini per part del responsable del contracte de l'Agència.

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 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 Coordinació amb altres equips

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

Aquesta coordinació 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 i 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 ciberseguretat.