Plec de prescripcions tècniques particulars que regeix l'acord marc per a la prestació de serveis d'auditories internes i auditories de certificacions per a l'Agència de Ciberseguretat de Catalunya

Lot 1: Auditories de certificació en l'ENS i evolució de l'OAT

Lot 2: Auditories internes d'estàndards normatius de seguretat

Exp. AM.03.2024

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Índex

1 Introducció

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

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

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

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

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

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

Les xifres fan paleses la necessitat de dotar-se de noves eines i de seguir ampliant el perímetre d'actuació. En aquest sentit, i alineat amb la nova Estratègia, l'Agència ampliarà el seu perímetre d'actuació i per tant, incrementar el nivell de protecció, resiliència i prevenció de més àmbits. Concretament, l'Agència, entre altres, ha de desplegar les seves capacitats i/o donar suport a diversos àmbits d'actuació, com són la Generalitat de Catalunya, l'Administració Local, les infraestructures crítiques i essencials, les universitats i centres de recerca, l'entorn hospitalari i assistencial, organismes públics i ciutadania (en

endavant, Àmbits d'Actuació), així com establir canals de col·laboració amb tot el sector de la ciberseguretat.

Amb una base legal sòlida i una visió estratègica clara, els acords marc facilitaran l'estandardització de processos i el desplegament de polítiques, mesures, solucions, iniciatives i programes de ciberseguretat, promouen la innovació i el talent, i contribuiran a un entorn digital més segur. A través d'una col·laboració efectiva entre l'Agència de Ciberseguretat, les administracions públiques, el sector privat incloses les PIMES que constitueixen un percentatge gran del teixit empresarial de Catalunya i la societat en general, es fomentarà el desenvolupament del sector de la ciberseguretat per garantir que Catalunya està ben posicionada per afrontar els reptes del present i del futur en el món digital. Aquests acords marc són, per tant, una peça clau en l'estratègia de Catalunya per construir un futur digital segur i resilient.

.

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

A efectes de la nova estratègia de contractació son rellevants les següents funcions de l'Agència:

- Serveis Corporatius s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació i la gestió de personal.
- Operació de la Seguretat du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció, resposta i recuperació de seguretat en la seva vessant més operativa i la seguretat corporativa.
- Desenvolupament d'Estratègia d'Àmbits té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes i iniciatives de seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- Producte s'ocupa d'identificar les necessitats i proposar noves idees i estratègies per a l'elaboració de nous productes generats per l'Agència o millora dels existents, i coordina l'execució del cicle de vida dels productes, des de la seva concepció fins a la seva retirada, incloent el disseny, desenvolupament, desplegament i control de qualitat.
- Centre d'Innovació i Competència en Ciberseguretat (CIC4Ciber) s'ocupa de la coordinació, cohesió i capacitat de l'ecosistema de Cibeseguretat de Catalunya, recolza el coneixement, sensibilització i conscienciació, i la innovació com a palanca de transformació i creixement del sector i fomenta la captació de forns i la internacionalització de l'entitat.

Certificacions en matèria de Ciberseguretat per desplegar totes les eines i processos vinculats al procés de certificació en ciberseguretat de les entitats, garantint sempre la independència necessària per la correcta execució d'aquests processos.

2 Descripció dels serveis objecte de l'Acord Marc

2.1 Context

En el marc del present plec tècnic en l'àmbit de l'auditoria de seguretat de la informació, actualment l'Agència desenvolupa una doble tasca com ens auditor. Per una banda, en data 4 d'agost de 2023 es va reconèixer a l'Agència com a Òrgan d'Auditoria Tècnica (OAT, en endavant) per part del Centre Criptològic Nacional (CCN, en endavant), concedint-li així, les competències per realitzar auditories de certificació de l'Esquema Nacional de Seguretat en el sector públic de Catalunya i emetre els certificats de conformitats derivats. Per altra banda, i de forma completament independent a la primera competència, també realitza auditories internes dels principals estàndards normatius de seguretat.

L'objecte de l'Acord Marc es donar resposta a totes les funcions que li son pròpies a l'Agència com OAT i ens auditor en l'àmbit del sector públic de Catalunya. Així, dita capacitat té una doble vessant (certificació i auditoria interna), que el present Acord Marc dona resposta a través de Lots en els quals s'estructura:

- **Lot 1**: Auditories de certificació en l'ENS i evolució de l'OAT
- **Lot 2**: Auditories internes d'estàndards normatius de seguretat

Les **companyies homologades que formin part del Lot 1**, com a requeriment per a desenvolupar funcions a l'Agència com a OAT, no poden participar en el Lot 2 d'aquest Acord Marc, ni en cap altre Acord Marc de l'Agència que contemplin activitats de consultoria, adequació, desenvolupament, assessorament, diagnòstic o d'altres activitats anàlogues que posin en risc la imparcialitat dels entorns que s'auditaran. A més, en els basats es podran demanar les justificacions i evidències pertinents a les companyies homologades per tal de demostrar que les persones proposades per dur a terme les activitats no han participat en activitats de la naturalesa anteriorment mencionada sobre els entorns i sistemes auditats, com a mínim en els darrers 2 anys, per garantir la completa objectivitat en les seves funcions. Addicionalment, serà necessari signar acords d'imparcialitat i confidencialitat de forma nominal.

Per altra banda, els **professionals que formin part del Lot 2**, no podran desenvolupar funcions d'altres Acords Marc de l'Agència que contemplin activitats de consultoria, adequació, desenvolupament, assessorament, diagnòstic o d'altres activitats anàlogues que posin en risc la imparcialitat dels entorns que s'auditaran. A més, en els basats es podran demanar les justificacions i evidències pertinents a les companyies homologades per tal de demostrar que les persones proposades per dur a terme les activitats no han participat en activitats de la naturalesa anteriorment mencionada sobre els entorns i sistemes auditats, com a mínim en els darrers 2 anys, per garantir la completa objectivitat en les seves funcions.

2.2 Elements bàsics d'execució

A banda de les funcions i tasques pròpies de cada servei, que s'especificarà en cadascun dels contractes basats del present acord marc (en endavant, Acord Marc) , els proveïdors adjudicataris hauran de desenvolupar tasques transversals i comunes que afectaran a la resta de serveis de l'Agència.

Es relacionen a continuació un seguit de tasques comunes en ambdós Lots. La determinació de l'objecte del contracte quedarà concretada en els contractes basats de l'Acord Marc.

- Alineació i orientació de la prestació del servei per a la consecució dels objectius estratègics de l'Agència.
- Manteniment actualitzat tota la informació i documentació relativa al propi servei i a la seva gestió, en la plataforma de gestió de la documentació que determini l'Agència, garantint que el coneixement resti a l'Agència tot i que finalitzi la prestació del servei.
- Participació en el els àmbits d'actuació de l'Agència, involucrant-se amb ells segons les necessitats de seguretat, el reporting requerit i les tipologies d'activitat.
- Participació en el model de relació amb els proveïdors d'altres contractes basats del mateix Acord Marc o d'altres Acords Marc, per tal d'assegurar la col·laboració fluida, la compartició d'informació i la gestió coherent i completa dels serveis extrem a extrem.
- Gestió les reunions i els conflictes que puguin aparèixer durant l'execució dels serveis.
- Portar a terme els plans d'actuació que facilitin la industrialització de l'activitat, segons el model presentat pel licitador a la seva proposta i segons la planificació pactada amb la Direcció de l'Agència.
- Realització el pla d'actuació periòdic amb les tasques planificades per les diferents iniciatives d'evolució o transformació per la pròpia operació del servei.
- Definició i gestió el pla de capacitat del servei, així com la resta de tasques assignades a les funcions de servei.
- Gestió els recursos materials dins l'àmbit de responsabilitat per al desenvolupament de les funcions descrites pel servei i per a la consecució dels objectius del mateix.
- Generació els indicadors, informes d'activitat i mesures de l'impacte d'aquesta activitat.
- Definició, creació, distribució i manteniment dels informes del servei i de risc derivats de l'activitat.
- Realització anàlisis i proves de les eines que es considerin oportunes per a la millora o industrialització del servei.
- Proposició millores, mantenir i, si s'escau construir les metodologies pròpies de treball del elements de servei objecte de licitació.
- Proposició accions que millorin la visibilitat del treball que produeix el servei tot enfocant a potenciar els resultats (informes, mètriques del servei, guies, infografies.) mitjançant propostes que permetin maximitzar-los en els diferents àmbits (Departaments, resta d'àrees, el CTTI, Comitè de Direcció de l'Agència,..) i fer que el es percebi el valor de les tasques realitzades.

- Durant l'execució del servei i a partir del coneixement adquirit, s'hauran de determinar, proposar i implantar de forma efectiva processos d'innovació que permetin millorar i/o renovar l'eficiència de solucions i processos, resoldre problemes complexos d'implantació, assolir millores en les metodologies emprades, permetre la renovació d'elements ja existents (eines, maquinari, etc.), així com adequar-se a noves necessitats i tecnologies que puguin esdevenir del propi procés d'innovació o transformació dels serveis.
- Participar a les iniciatives d'innovació de l'entitat aportant-hi la visió, coneixement i experiència des de la perspectiva de l'operativa del servei per a la identificació d'oportunitats d'innovació, i la conceptualització i avaluació de solucions. Aportar també la capacitat operativa i de mesura i avaluació del servei per al desplegament, en l'àmbit del servei, de pilots i solucions associades a aquestes iniciatives.

2.3 Elements concrets d'execució

2.3.1 Serveis específics Lot 1 – Auditories de certificació en l'ENS i evolució de l'OAT

En aquest Lot es duran a terme auditories de certificació en l'Esquema Nacional de Seguretat (ENS, en endavant) en el sector públic de Catalunya, s'emetran els certificats de conformitat derivats, i es vetllarà pel manteniment i l'evolució de l'OAT de l'Agència, de forma alineada amb els criteris establerts pel CCN.

Les auditories de certificació en l'ENS es podran realitzar sobre qualsevol dels Àmbits d'Actuació de l'Agència de Ciberseguretat de Catalunya, implicant en alguns casos un desplaçament.

A continuació s'exposen les funcions que s'emmarquen dins el Lot 1 de l'Acord Marc i que podran ser objecte dels contractes derivats corresponents. Aquestes tasques son enunciatives i, en cap cas es poden considerar limitatives, per tant, es podran ampliar i concretar en els posteriors contractes basats:

- Realització de les auditories de certificació en tot el seu cicle de vida: planificació, pla d'auditoria, auditoria en sí (revisió d'evidències), valoració dels incompliments, informe de resultats, valoració dels PAC (plans d'acció correctius), etc.
- Vigilància del bon ús de distintius i certificats de les entitats auditades per l'Agència.
- Manteniment i evolució del sistema de gestió de la imparcialitat de l'OAT, basat en l'estàndard ISO17065, i de tots els documents normatius, metodologies, plantilles, registres, etc. que el conformen.
- Industrialització i automatització dels processos que es desenvolupen des de l'OAT, per fer front a l'escalabilitat de les seves funcions.
- Manteniment dels repositoris documentals de l'OAT
- Suport a l'Agència en la re-acreditació com a OAT.
- Assegurament de la imparcialitat dels equips.
- Generació d'indicadors de compliment en els Àmbits d'Actuació.
- Formació i la capacitació contínua en l'ENS.

Metodologies de treball

L'Agència, com a OAT, ha de vetllar per l'alineament i aplicació de les guies, normatives i metodologia del CCN en quant a la realització d'auditories de certificació de conformitat amb l'ENS. En concret, la seva metodologia es basa en la darrera versió de la guia CCN-CERT IC-01/19 en la qual s'estableixen els criteris generals per a l'auditoria i la certificació dels sistemes d'informació de l'àmbit d'aplicació de l'ENS.

Les companyies homologades, hauran de ser coneixedores i saber aplicar les guies CCN-STIC per poder realitzar les auditories de certificació, així com disposar del coneixement adequat de seguretat en sistemes d'informació per poder auditar els diferents àmbits independentment de la tecnologia utilitzada.

A més, les companyies homologades hauran de ser capaces de presentar la seva metodologia de treball per garantir:

- La transparència, la qualitat i l'eficiència en el procés d'auditoria de certificació de conformitat en l'ENS.
- Que l'equip coneix i es manté actualitzat en tot moment amb les guies CCN-STIC que apliquen per a la realització de les auditories,
- La formació i capacitació contínua de l'equip.
- La coordinació de manera eficient i eficaç dels diferents equips auditors tenint en compte que poden haver diverses auditories en paral·lel, assegurant en tot moment la professionalitat, la qualitat i els terminis.
- L'escalabilitat del servei per fer front a un volum creixent de certificacions (i re-certificacions) en tots els Àmbits d'Actuació.

Equip

L'Agència com a OAT ha de complir, de forma estricta, amb requeriments d'imparcialitat i confidencialitat per assegurar que els certificats emesos són fiables, i les dades dels seus clients es troben protegides. Per a fer-ho, l'Agència ha desplegat un sistema de gestió basat en la norma ISO 17065. A més, per donar compliment, l'equip dedicat que les companyies homologades presentin als basats, hauran de complir també, amb tots aquests requisits d'imparcialitat i confidencialitat.

En cap cas els integrants de l'equip auditor proposats als basats hauran d'haver participat o dut a terme responsabilitats prèvies en el sistema d'informació auditat, o bé haver donat cap tipus d'assessorament o consultoria, per a aquest sistema, en el procés d'implementació dels requisits de l'ENS, almenys en els 2 últims anys.

Tots els integrants de l'equip auditor hauran d'haver signat, abans de començar a intervenir en auditories de Certificació de la Conformitat amb l'ENS, un acord de confidencialitat i imparcialitat, que garanteixi el seu deure de secret davant la informació a la qual tinguin accés, o elaborin, durant les auditories, i que garanteixin l'absència de conflicte d'interès.

L'Agència, dins de les seves funcions com a OAT, disposa de personal intern que realitza les funcions de Responsable Tècnic i Revisor d'Expedients. Es buscarà que les companyies homologades presentin principalment equips d'auditoria, i personal expert que permeti evolucionar i transformar l'OAT.

A títol enunciatiu i no limitatiu es defineixen els rols i les funcions que es podran sol·licitar en els posteriors contractes basats de manera no acumulativa:

- **Responsable d'empresa homologada:**

    - Punt de contacte central de l'empresa homologada respecte a la gestió de l'Acord Marc, amb visió global i transversal. Encarregat de garantir que el servei es duu a terme d'acord amb les necessitats del client, coordinant els recursos del servei i assumint les decisions segons necessitats del client, en qualsevol àmbit que afecti la gestió del servei.
    - Encarregat d'assegurar la col·laboració amb les empreses adjudicatàries d'altres contractes amb qui s'ha de relacionar per tal de millorar el servei de negoci final.
    - Realitzar funcions de direcció global. Vetllar per la correcta coordinació dels serveis i projectes dels contractes basats, tot garantint-ne l'assoliment dels objectius. Garantir que els equips de gestió siguin els més adequats per l'assoliment dels objectius.
    - Participar en els òrgans de govern del contracte d'acord amb el Model de Relació.

    Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional expert amb altes capacitats de lideratge i de comunicació.

- **Coordinador/Cap de Servei:**

    - Lideratge del basat, planificació, supervisió i coordinació dels diferents perfils implicats en la prestació de serveis del contracte.
    - Actuar com a enllaç entre la companyia homologada i els diferents responsables implicats de l'Agència.
    - Assegurar que tot el personal de la companyia homologada que prestarà serveis, passi per un pla de conscienciació i formació en matèria de seguretat, l'ENS i auditories de sistemes.
    - Assegurar que tot el personal de la companyia homologada que hagi de participar en les auditories de certificació signin un Acord d'Imparcialitat Individual.
    - Garantir, liderar i impulsar el compliment del marc normatiu de seguretat aplicable dins la seva organització, assegurant la correcta implantació dels nivells de seguretat i les seves corresponents mesures (tècniques, organitzatives, i jurídiques); així com les directrius en matèria de seguretat establertes per l'Agència de Ciberseguretat.
    - Realitzar el reporting periòdic de l'evolució i resultats del servei i assegurar la informació regular a l'Agència de Ciberseguretat segons els terminis marcats.

    Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional amb àmplia experiència en gestió de serveis i gestió d'equips, amb capacitats de lideratge i de comunicació.

- **Auditor Expert de l'ENS:**

    - Encarregat de planificar, fer seguiment, prestar suport, acompanyament i assessorament en la gestió de les auditories, i la millora de l'eficiència de les activitats i processos.

- Responsable i supervisor de tot el procés d'auditoria i de l'equip d'auditoria involucrat, participant activament també en l'execució de la mateixa, i assegurant la qualitat de l'informe resultant.
- Encarregat de confeccionar el pla d'auditoria, de forma prèvia a l'inici d'aquesta, que haurà d'establir amb claredat la responsabilitat i assignació de funcions a cada integrant de l'equip auditor.
- Analitzar i comprendre els objectius i abast de l'auditoria, així com les normes i regulacions aplicables, i detectar la necessitat de requerir de perfils experts especialistes quan les característiques de l'auditoria requereixin de coneixements específics.
- Assegurar l'exactitud de totes les troballes observades i la conclusió final.
- Preservar les evidències d'auditoria seguint els repositoris i eines de l'Agència.
- Mantenir una comunicació efectiva tant amb l'equip d'auditoria com amb l'organització auditada, assegurant-se que es transmeti la informació adequada en cada etapa del procés.
- Identificar millores en els processos del servei.

Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional amb àmplia experiència i coneixements en l'àmbit de la realització d'activitats relacionades amb auditories normatives i auditories de seguretat, ampli coneixement en l'ENS, i amb habilitats de gestió de projectes, presentació i comunicació.

- **Auditor de l'ENS:**

  - Avaluar i verificar el grau de compliment de les mesures de seguretat en les entitats auditades.
  - Realitzar proves i verificacions tècniques per validar la correcta configuració i funcionament dels sistemes i tecnologies utilitzades.
  - Elaborar els informes d'auditoria, així com qualsevol altra documentació relacionada amb el procés d'auditoria, i documentar amb exactitud les evidències recopilades.

  Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional amb coneixements en seguretat de la informació i normativa de seguretat, incloent l'ENS, i preparació prèvia en auditories de sistemes d'informació.

- **Expert en sistemes de gestió:**

  - Manteniment i evolució del sistema de gestió de la imparcialitat de l'OAT, basat en estàndards ISO, i de tots els documents normatius, metodologies, plantilles, registres, etc. que el conformen.
  - Avaluar i millorar les metodologies utilitzades amb l'objectiu de buscar formes més eficients i efectives de dur a terme les activitats, assegurant la qualitat, la eficiència i la satisfacció del client.
  - Identificar tasques i activitats que es puguin realitzar de manera automatitzada, avaluant les tasques existents, identificant les oportunitats d'automatització.
  - Vetllar per l'ús correcte dels distintius i certificats vigents de les entitats seguint les guies del CCN.

  Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional amb experiència en el manteniment, assessorament i millora de sistemes de gestió. Podrà, així mateix, actuar en qualitat d'algun dels altres rols, sempre que reuneixi els requisits necessaris i que l'Agència així ho consideri.

- **Experts tècnics:**

    - Proporcionar habilitats i coneixements especialitzats i assessorament tècnic, tant a la gestió de l'OAT com durant el procés d'auditoria quan l'entorn tecnològic i normatiu ho requereixi (p.e. entorns cloud, blockchain, intel·ligència artificial, aplicació de normativa molt específica, automatització de processos, programació d'scripts, etc.).

Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional amb experiència en l'àmbit d'expertesa en què es requereixi la seva participació. Podrà, així mateix, actuar en qualitat d'algun dels altres rols, sempre que reuneixi els requisits necessaris i que l'Agència així ho consideri.

2.3.2 Serveis específics Lot 2 – Auditories internes d'estàndards normatius de seguretat

En aquest Lot es duran a terme la realització d'auditories internes en els diferents Àmbits d'Actuació de l'Agència dels principals estàndards normatius de seguretat (o d'altres que puguin ser d'aplicació per a les funcions de l'Agència sobre els Àmbits d'Actuació), com per exemple i de forma no limitativa: l'ENS, la ISO27001, la ISO22301 i la Protecció de dades, entre d'altres. També es podran requerir auditories internes de la norma ISO17065 sobre el servei de l'OAT de l'Agència per assegurar la imparcialitat i afavorir la millora contínua del seu sistema de gestió de la imparcialitat.

Per fer-ho, és necessari la realització de totes les tasques associades al cicle de vida d'aquestes auditories internes, així com les tasques de gestió i transversals pel seu correcte funcionament i gestió adequada.

A continuació s'expliquen les funcions que s'emmarquen dins el Lot 2 de l'Acord Marc i que podran ser objecte dels contractes derivats corresponents. Aquestes tasques son enunciatives i, en cap cas es poden considerar limitatives, per tant, es podran ampliar i concretar en els posteriors contractes basats:

- Realització de les auditories internes en tot el seu cicle de vida: planificació, pla d'auditoria, execució de l'auditoria (reunions i visites, identificació de requeriments d'aplicació, revisió d'evidències, etc.), valoració dels incompliments, informe de resultats, valoració dels PAC (plans d'acció correctius), etc.
- Manteniment i millora de les plantilles dels lliurables i tota la documentació associada.
- Evolució de la metodologia de treball i de gestió.
- Manteniment dels repositori documentals: d'evidències, registre d'auditories internes, etc.
- Generació d'indicadors de compliment en els Àmbits d'Actuació.
- Formació i capacitació contínua.

Metodologies de treball

Per garantir l'efectivitat i la qualitat de les auditories internes, les companyies homologades han de demostrar que disposen de coneixements sòlids i de metodologies pròpies madures per realitzar les auditories internes pels diferents estàndards normatius.

Les companyies homologades hauran d'exhibir una comprensió integral de les normatives i estàndards rellevants, així com la capacitat d'adaptar la seva metodologia a les especificitats de cada auditoria interna. Per altra banda, han de disposar del coneixement adequat de seguretat en sistemes d'informació per poder auditar els diferents àmbits independentment de la tecnologia utilitzada.

A més, les companyies homologades hauran de ser capaces de presentar la seva metodologia de treball per garantir:

- La transparència, la qualitat i l'eficiència en el procés d'auditoria interna.
- La formació i capacitació contínua de l'equip.

- Que l'equip coneix i es manté actualitzat en tot moment amb els diferents estàndards que apliquen per a la realització de les auditories internes.
- Presentar de forma adequada els resultats de les auditories internes d'acord amb el sistema i la metodologia i eines de valoració i de reportat de l'Agència.
- La coordinació de manera eficient i eficaç dels diferents equips auditors tenint en compte que poden haver diverses auditories internes en paral·lel, assegurant en tot moment la professionalitat, la qualitat i els terminis.
- Les millores del procés i d'altres peticions per tal de garantir-ne la màxima eficiència i l'ajustament a les necessitats de l'Agència, tenint en compte l'escalabilitat de les activitats.

Equip

L'equip d'auditoria interna estarà conformat per professionals altament capacitats i especialitzats en l'àmbit de la seguretat de la informació i el compliment normatiu, amb experiència significativa en auditories de seguretat de la informació i normativa. La diversitat d'habilitats dins de l'equip garantirà la col·laboració, la comunicació efectiva i la millora contínua que seran pilars fonamentals en l'execució d'aquestes auditories.

En cap cas els integrants de l'equip auditor proposats als basats hauran d'haver participat o dut a terme responsabilitats prèvies en el sistema d'informació auditat, o bé haver donat cap tipus d'assessorament o consultoria, per a aquest sistema, almenys en els dos últims anys. Caldrà garantir en tot moment la imparcialitat i confidencialitat a les auditories que es duran a terme.

A títol enunciatiu i no limitatiu es defineixen els rols i les funcions que es podran sol·licitar en els posteriors contractes basats de manera no acumulativa:

- **Responsable d'empresa homologada:**

    - Punt de contacte central de l'empresa homologada respecte a la gestió de l'Acord Marc, amb visió global i transversal. Encarregat de garantir que el servei es duu a terme d'acord amb les necessitats del client, coordinant els recursos del servei i assumint les decisions segons necessitats del client, en qualsevol àmbit que afecti la gestió del servei.
    - Encarregat d'assegurar la col·laboració amb les empreses adjudicatàries d'altres contractes amb qui s'ha de relacionar per tal de millorar el servei de negoci final.
    - Realitzar funcions de direcció global. Vetllar per la correcta coordinació dels serveis i projectes dels contractes basats, tot garantint-ne l'assoliment dels objectius. Garantir que els equips de gestió siguin els més adequats per l'assoliment dels objectius.
    - Participar en els òrgans de govern del contracte d'acord amb el Model de Relació.

    Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional expert amb altes capacitats de lideratge i de comunicació.

- **Coordinador/Cap de Servei:**

    - Lideratge del basat, planificació, supervisió i coordinació dels diferents perfils implicats en la prestació de serveis del contracte.

- Actuar com a enllaç entre la companyia homologada i els diferents responsables implicats de l'Agència.
- Assegurar que tot el personal de la companyia homologada que prestarà serveis, passi per un pla de conscienciació i formació en matèria de seguretat, els diferents estàndards a auditar i auditories de sistemes.
- Garantir, liderar i impulsar el compliment del marc normatiu de seguretat aplicable dins la seva organització, assegurant la correcta implantació dels nivells de seguretat i les seves corresponents mesures (tècniques, organitzatives, i jurídiques); així com les directrius en matèria de seguretat establertes per l'Agència de Ciberseguretat.
- Realitzar el reporting periòdic de l'evolució i resultats del servei i assegurar la informació regular a l'Agència de Ciberseguretat segons els terminis marcats.

Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional amb àmplia experiència en gestió de serveis i gestió d'equips, amb capacitats de lideratge i de comunicació.

- **Auditor Expert en Ciberseguretat**:

  - Encarregat de planificar, fer seguiment, prestar suport, acompanyament i assessorament en la gestió de les auditories internes, i la millora de l'eficiència de les activitats i processos.
  - Responsable i supervisor de tot el procés d'auditoria interna i de l'equip d'auditoria involucrat, participant activament també en l'execució de la mateixa, i assegurant la qualitat de l'informe resultant.
  - Encarregat de confeccionar el pla d'auditoria interna, de forma prèvia a l'inici d'aquesta, que haurà d'establir amb claredat la responsabilitat i assignació de funcions a cada integrant de l'equip auditor.
  - Analitzar i comprendre els objectius i abast de l'auditoria interna, així com les normes i regulacions aplicables, i detectar la necessitat de requerir de perfils experts especialistes quan les característiques de l'auditoria requereixin de coneixements específics.
  - Assegurar l'exactitud de totes les troballes observades i la conclusió final.
  - Preservar les evidències d'auditoria seguint els repositoris i eines de l'Agència.
  - Mantenir una comunicació efectiva tant amb l'equip d'auditoria interna com amb l'organització auditada, assegurant-se que es transmeti la informació adequada en cada etapa del procés.
  - Identificar millores en els processos del servei.

  Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional amb àmplia experiència i coneixements en l'àmbit de la realització d'activitats relacionades amb auditories normatives i auditories de seguretat, ampli coneixement en els diferents estàndards a auditar, i amb habilitats de gestió de projectes, presentació i comunicació

- **Auditor en Ciberseguretat**:

  - Avaluar i verificar el grau de compliment de les mesures de seguretat en les entitats auditades.
  - Realitzar proves i verificacions tècniques per validar la correcta configuració i funcionament dels sistemes i tecnologies utilitzades.

- Elaborar els informes d'auditoria interna, així com qualsevol altra documentació relacionada amb el procés d'auditoria interna, i documentar amb exactitud les evidències recopilades.

Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional amb coneixements en seguretat de la informació i normativa de seguretat, incloent els diferents estàndards a auditar, i preparació prèvia en auditories de sistemes d'informació.

- **Experts tècnics**:

  - Proporcionar habilitats i coneixements especialitzats i assessorament tècnic, durant el procés d'auditoria quan l'entorn tecnològic i normatiu ho requereixi (p.e. entorns cloud, blockchain, intel·ligència artificial, aplicació de normativa molt específica, automatització de processos, programació d'scripts, etc.)
  - Podrà així mateix actuar en qualitat d'algun dels altres rols, sempre que reuneixi els requisits necessaris i que l'Agència així ho consideri.

Atenent a les funcions anteriors, es requerirà que aquest perfil sigui un professional amb experiència en l'àmbit d'expertesa en què es requereixi la seva participació. Podrà, així mateix, actuar en qualitat d'algun dels altres rols, sempre que reuneixi els requisits necessaris i que l'Agència així ho consideri.

3 Condicions d'execució del servei

3.1 Equip de treball

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

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

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.
- Habilitat per identificar, analitzar i resoldre problemes.
- Capacitat de treball sota pressió.
- Coneixement de català, castellà i d'anglès, parlat i escrit.
- Ampli coneixement legal, tecnològic i de negoci de seguretat informàtica i de l'entorn de l'administració pública.
- Altres necessaris per al bon desenvolupament dels serveis.

La prestació del servei ha de ser proporcionada amb l'estructura i el nombre de recursos humans amb els coneixements necessaris per poder donar el servei amb garanties d'èxit en la situació inicial, durant la transició i en l'execució, donant resposta a les funcions i requisits del servei i als diferents processos a realitzar. L'Agència revisarà i validarà els currículums presentats per l'adjudicatari del contracte basat des de la primera incorporació.

A causa de l'evolució dels serveis i la tecnologia, és probable que addicionalment a la formació que puguin rebre els perfils assignats, s'hagin d'incorporar nous perfils no explícitament definits tal com queda definit en el present Acord Marc. En aquest cas la concreció del perfil es determinarà en el contracte basat.

L'empresa adjudicatària del contracte basat, per requisits de seguretat i control, haurà de lliurar a l'Agència una relació actualitzada dels professionals assignats al servei amb les dades que es puguin identificar, usant mitjans i formats de l'Agència; amb la periodicitat que s'estableixi en els contractes basats.

Aquesta contractació no crearà cap vinculació laboral entre el personal que presti el servei objecte del contracte i l'Agència. A l'extinció dels contractes basats, no podrà produir-se en cap cas la consolidació de les persones que hagin prestat el servei objecte del contracte com a personal l'Agència.

3.2 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte basat el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o

per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies laborables a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència a l'empresa adjudicatària del contracte basat. L'adjudicatari haurà de presentar en un termini màxim de 10 dies laborables a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució. Si l'objecte del contracte basat ho requereix, aquest aspecte es podrà concretar en aquest.

3.3 Control de rotació

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

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

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

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

3.4 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions com a Centre d'Innovació i Competència en Ciberseguretat (CIC4Cyber) i, especialment, l'impuls de la transformació fonamentada en el coneixement col·laboratiu, la coordinació de l'ecosistema de ciberseguretat i la voluntat per la innovació continua, es requereix que les empreses homologades registrin tot el coneixement que disposin i es generi en la contractació basada que derivi del present Acord Marc d'acord amb les directrius del CIC4Cyber.

A tal efecte, la companyia homologada 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.

Sens perjudici de tot l'anterior, quan la naturalesa del servei objecte de la contractació basada així ho requereixi l'Agència podrà demanar a l'empresa adjudicatària la realització d'actuacions addicionals per a garantir la transmissió del coneixement generat

3.5 Seguretat Corporativa

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

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- Facilitar l'accés en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de l'Agència (sigui o no per l'exercici de la seva funció).
- Acceptar les normes i polítiques que estableix l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.
- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'àrea de Mitjans Tècnics per fer el desplegament de polítiques i controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.
- Els equips, així com la informació resident dels mateixos serà sempre custodiada per l'Agència.
- Garantir l'estabilitat dels equips (reduint al mínim la rotació de personal).
- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (ENS, LOPDGDD, GDPR, LSSI, etc.).

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

3.6 Control de Gestió

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

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

- Seguiment dels riscos.
- Seguiment del consum de recursos.
- Imputació de temps i activitats.
- Assignació de tasques a persones.
- Memòria d'activitat del contracte.
- Facturació i Conformació de factures.

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

3.7 Formació

El personal de les empreses homologades l'adjudicatari disposarà de la formació adequada per al desenvolupament de les seves tasques. Sens perjudici d'aquesta qüestió el personal de l'empresa adjudicatària del contracte basat realitzarà, si s'escau, formació continuada per tal de garantir l'actualització dels seus coneixements així com l'adquisició de nou coneixement que pugui ser de valor pels serveis de l'Agència.

3.8 Contingència

Els licitadors hauran de proveir un pla de contingència, en cas de desastre de les instal·lacions principals, en unes instal·lacions alternatives (centre de gestió secundari) propietat del licitador, que inclouran:

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

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

3.9 Validació de la Documentació

L'Agència és la propietària de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris i el seu personal i subcontractistes 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 que coordini el servei contractat a l'adjudicatari 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 el present acord marc, o en el seu cas en el posterior contracte basat.

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

3.10 Metodologia, estàndards i lliurables

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

3.11 Seguretat

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

3.11.1 Deure de confidencialitat

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

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

3.11.1. Dades de caràcter personal

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

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

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

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

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

3.11.3. Capacitat tècnica

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

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

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

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

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

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

3.11.5. Interconnexions

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

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

3.11.6. Verificació del compliment i auditoria

L'Agència es reserva el dret a verificar i auditar, amb mitjans propis o de tercers, el compliment de les mesures de seguretat requerides en base al marc legal de ciberseguretat i al marc intern per als sistemes d'informació emprats per a l'execució del contracte, en el moment i amb la periodicitat que s'estimi convenient. L'Agència podrà requerir el seguiment dels plans d'acció derivats d'aquestes verificacions i auditories. L'empresa adjudicatària del contracte basat haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en relació a aquest model de compliment, donant resposta en els terminis marcats per l'Agència de Ciberseguretat. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència de Ciberseguretat.

3.11.7. Incidents de seguretat

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

per a la seva gestió i notificació als organismes competents per part de l'Agència de Ciberseguretat.

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

3.11.8. Accés a la informació

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

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

3.12 Integració amb altres equips

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

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

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

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

3.13 Compromís amb el talent femení

El febrer de l'any 2022 l'Agència va aprovar el Pla Estratègic de Dones en Ciberseguretat a l'àmbit de Catalunya, el qual es troba alineat amb les directrius i estratègies impulsades pel Govern de la Generalitat de Catalunya, com ara el Pla Estratègic de Polítiques d'Igualtat de Gènere, l'Estratègia de Ciberseguretat de Catalunya i el Pla Dona TIC, que té com finalitat fomentar la igualtat de gènere en el sector de la Ciberseguretat i, en conseqüència, incrementar el número de dones que es dediquen a la Ciberseguretat.

Per deixar palès aquest compromís i voluntat per impulsar iniciatives que permetin donar a conèixer i captar el talent femení, quan la naturalesa del servei objecte de la contractació basada ho faci possible l'Agència podrà preveure criteris per fomentar el talent femení i la seva presència en el camp de la Ciberseguretat.

3.14 Compromís amb el talent i la inclusió

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

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

Per deixar palès aquest compromís i voluntat, quan la naturalesa del servei objecte de la contractació basada ho faci possible l'Agència podrà preveure criteris per fomentar la inclusió en la generació de talent i la seva presència en el camp de la Ciberseguretat.

4 Model de governança

4.1 Objectiu

El model de governança de serveis de l'Agència té com a objectiu gestionar de manera eficient i eficaç els recursos disponibles, per tal de garantir el millor servei que doni resposta a necessitats estratègiques, de seguretat i operatives dels departaments i entitats a què l'Agència presta serveis de ciberseguretat.

Aquest model pretén assolir els següents objectius estratègics principals:

- **Qualitat**: Garantir la qualitat en la prestació de serveis i la satisfacció dels usuaris, segons les necessitats dels diferents col·lectius.
- **Eficiència**: Optimitzar l'ús dels recursos gràcies a la cerca d'eficiències, sinergies i optimització.
- **Innovació**: Transformar i innovar a l'administració d'acord amb l'estratègia transversal de ciberseguretat de l'Agència i de les TIC de la Generalitat.
- **Seguretat**: Garantir que tots els serveis prestats incorporen les mesures de seguretat necessàries d'acord a les directrius de l'Agència i són els més adients per fer front a possibles incidents de ciberseguretat.
- **Coneixement**: Generar coneixement a partir de la informació gestionada pels serveis, per donar resposta a les necessitats i a la presa de decisions en l'àmbit del negoci de l'Agència.

4.2 Abast

El model de prestació de serveis de ciberseguretat està definit com un escenari multi proveïdor amb externalització de serveis tecnològics. El responsable de l'estratègia i el govern és l'Agència i el model de governança estableix el model de relació entre els diferents actors implicats (Agència, entitats i proveïdors). Així doncs, aquest model de relació estableix les activitats, entrades i sortides dels diferents comitès que el configuren, així com els mecanismes de seguiment per assegurar que la governança es duu a terme de la manera més eficaç i eficient possible.

4.3 Principis i premisses

Per realitzar la governança dels serveis, l'adjudicatari de cada contracte basat seguirà la metodologia que s'hagi definit al respectiu plec i acordat en la fase d'establiment del servei per tal que la gestió dels serveis i el seu seguiment siguin àgils, efectius i eficients.

El Cap de Servei del contracte basat de l'adjudicatari reportarà directament als responsables del contracte de l'Agència, l'estat, l'evolució i els riscos dels serveis objecte del contracte, seguint el model de relació establert a cada basat i que estarà format per diferents nivells d'interlocució.

4.3.1 Alineació amb objectius estratègics

La Direcció de l'Agència estableix una sèrie d'objectius a nivell estratègic basats en la visió, missió i valors de l'entitat, i els responsables que coordinen els serveis estableixen

quins resultats clau contribuiran a aquests objectius i a quin equip involucrar per assolir-los. Aquests vindran fixats per una sèrie d'indicadors que permetin mesurar el grau de compliment al llarg del temps dels objectius. Aquest objectius seran mesurables, específics, clars, coherents, realistes i oportuns. D'aquesta manera contribueixen a materialitzar l'estratègia, ajudar a establir les fites i avaluar el compliment, i a crear una alineació de tota l'organització.

El model de governança que segueixi cada adjudicatari d'un contracte basat haurà de facilitar aquest alineament estratègic i garantir-ne el seguiment i l'adaptació a les necessitats i objectius de l'Agència.

4.4 Gestió de la demanda

L'interlocutor de la demanda de serveis de Ciberseguretat és l'Agència. Per tant, l'Agència és qui canalitzarà i gestionarà aquesta demanda cap als diferents proveïdors que presten els serveis a través dels contractes basats.

Aquesta canalització (gestió de la demanda) es tractarà mitjançant la gestió de projectes (per les iniciatives i necessitats), i la gestió de serveis (per les peticions i incidències).

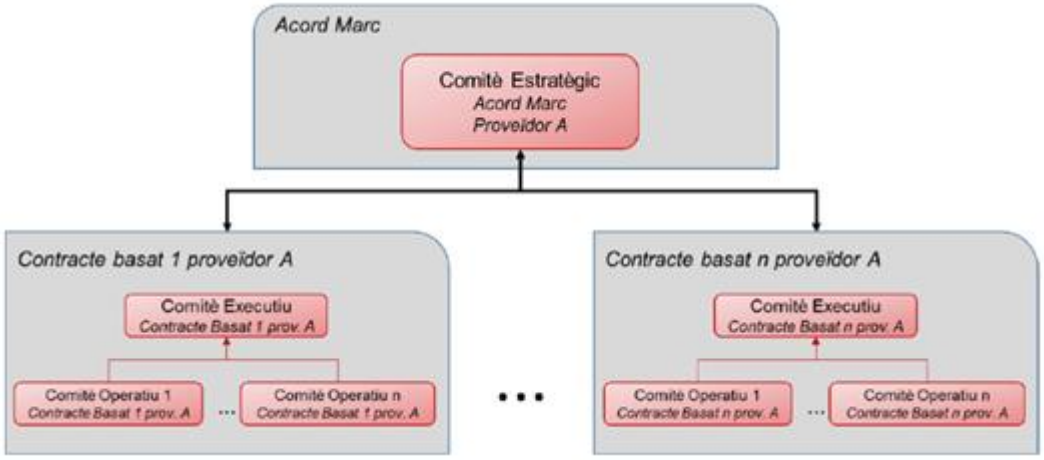
En cas que el proveïdor rebi directament alguna sol·licitud d'iniciativa o necessitat, per part d'un departament o entitat, haurà de ser redireccionada a l'òrgan gestor de l'Agència encarregat de la demanda. Per les peticions i incidències, el grau d'automatització determinarà la recepció directa d'aquestes pel proveïdor, mitjançant les eines de suport a la gestió dels serveis de l'Agència.

4.5 Òrgans de Gestió (Comitès)

El model de relació es basa en establir els comitès i el funcionament d'aquests, per assegurar el compliment dels requeriments de les condicions d'execució del serveis descrites en aquest plec i dels contractes basats que se'n derivin. Aquests comitès tindran també com a funció executar els mecanismes per ajustar aquestes condicions d'acord amb l'evolució de les necessitats de servei.

Les empreses homologades assumiran aquest model de relació i l'estructura de comitès que s'implementarà per la governança específica dels serveis objecte d'aquest Acord Marc.

En aquest apartat es descriuen tant el model de relació de l'Acord Marc com el dels seus contractes basats. Els comitès que conformen aquests models de relació i el seu flux d'informació es mostren a la següent figura:



4.5.1 Comitè Estratègic Acord Marc

El model de relació a nivell d'Acord Marc es basarà en un únic comitè el qual serà l'òrgan central de la relació entre l'Agència i cada una de les empreses homologades i en el seu cas, adjudicatàries dels contractes basats.

Els assistents a aquest comitè per part de l'adjudicatari hauran de tenir capacitat decisòria sobre els compromisos i acords que es prenguin en el comitè.

Aquest comitè es farà de manera conjunta per tots els contractes basats adjudicats a un mateix proveïdor, independentment del lot al que pertanyin.

Títol	
Comitè Estratègic de l'Acord Marc	
Participants	
Agència	***Empresa homologada***
- Responsable de Contracte de l'Acord Marc - Direcció de l'Agència - Responsables del servei (si escau) - Altres assistents (si escau)	- Responsable d'empresa homologada - Caps de serveis - Responsables dels àmbits d'execució específics / Coordinadors (si escau)
Objectius	
- Marcar les directrius estratègiques - Identificar les directrius tàctiques a traslladar als contractes basats. - Realitzar el seguiment del conjunt d'activitats desenvolupades en els diferents contractes basats durant en el període, orientat especialment a l'assoliment dels objectius i eficiències plantejades pel proveïdor. - Realitzar el seguiment i control global de l'operació i provisió dels serveis d'acord als acords de nivells de servei definits al diferents contractes basats, fent èmfasi en els eventuals desviaments. - Fer el seguiment de les incidències en el compliment de les obligacions contractuals dels diferents contractes basats. - Fer seguiment globals del model econòmic dels diferents contractes bastats, fent èmfasi en els eventuals desviaments. - Revisar i proposar les penalitzacions per incompliment del servei dels diferents contractes basats per escalar-les a l'òrgan de contractació. - Identificar oportunitats de millora de la qualitat global del servei. - Planificar, prioritzar i revisar les iniciatives en curs. - Planificar, prioritzar i revisar les activitats amb impacte transversal.	

Entrades	Sortides
- Informes i quadres de comandament dels contractes basats. - Actes comitès executius dels contractes basats - Decisions a prendre	- Acta (signada entre les parts) - Decisions preses - Directrius a traslladar pels contractes basats. - Propostes a l'Òrgan de Contractació
Periodicitat	
A petició de l 'Agència	

Amb independència del disseny organitzatiu de cada contracte basat d'acord marc, l'equip de treball a nivell global d'acord marc estarà composat, com a mínim, per un responsable (comú per a tots els lots) per a cada empresa homologada.

Responsable d'empresa homologada

Aquesta figura és única per empresa homologada. És la figura de referència i el darrer responsable de la prestació del conjunt de serveis i projectes del proveïdor. Aquesta figura es mantindrà durant tota la vida del contracte o contractes entre l'Agència i el proveïdor, en la gestió comercial, durant la provisió del servei i fins la devolució del mateix. Ha de ser garant de l'existència dels mecanismes de relació en la seva organització per portar a terme els acords presos entre l'Agència i el proveïdor. En cas que es produeixin canvis en l'abast i/o cost dels serveis que impliquin una modificació contractual, és el responsable de vehicular-ho.

Entre les seves responsabilitats podem destacar:

- Consolidar i aportar a l'Agència les informacions tant objectives com subjectives; valorades (informació fiable i de qualitat i analitzada en base al coneixement del model) que permetin la presa de decisions operatives i estratègiques al llarg de la vida de l'Acord Marc.
- Ser l'interlocutor principal amb l'Agència en matèria jurídica-legal per tots els serveis/contractes prestats per l'adjudicatari. Serà el responsable de la formalització de les interpretacions realitzades respecte els contractes vigents, quan aquestes impliquin modificacions contractuals.
- Ser el responsable de que l'Agència rebi els informes de gestió acordats, tant amb indicadors econòmic-financers com d'altres, així com de realitzar el seguiment del model econòmic acordat amb l'adjudicatari.
- Ser el responsable de que el proveïdor faciliti la informació relativa al procés de facturació, segons el model i format definit per l'Agència, així com col·laborar en el procés de la conciliació.

El model de relació a nivell de contracte basat es durà a terme en dos únics comitès que gestionaran el nivell executiu i el nivell operatiu dels contractes basats.

4.5.2 Comitè Executiu Contractes Basats

Aquest comitè executiu es durà a terme per cada un dels contractes basats adjudicats. Servirà per realitzar el seguiment i control global de la provisió dels serveis d'acord amb els acords de nivells de servei definits en cada basat, traslladar les directrius tàctiques al nivell operatiu, planificar, prioritzar i revisar les activitats i fer el seguiment de les obligacions contractuals i del model econòmic del contracte basat.

Títol

Comitè Executiu de Contracte Basat	
Participants	
Agència	***Proveïdor***
- Responsable del Contracte Basat - Responsable/s del servei - Responsable de Contracte de l'Acord Marc (si escau) - Altres assistents (si escau)	- Cap de serveis del contracte - Responsables dels àmbits d'execució específics (si escau) - Responsable d'empresa homologada (si escau)
Objectius	
- Marcar les directrius tàctiques - Identificar les directrius a traslladar al nivell operatiu. - Realitzar el seguiment del conjunt d'activitats desenvolupades en el període, orientat especialment a l'assoliment dels objectius i eficiències plantejades pel proveïdor. - Realitzar el seguiment dels ANS associats als contracte basat, fent èmfasi en els desviaments. - Revisió i estat de situació dels aspectes més rellevants del marc del contracte basat (riscos, incidents del període...). - Fer el seguiment de les obligacions contractuals del basat. - Fer el seguiment del model econòmic. - Revisar i proposar les penalitzacions per incompliment del servei i escalar-les a l'òrgan de contractació. - Identificar possibles modificacions del contracte basat i proposar-les a l'òrgan de contractació. - Acordar els quadres de comandament del contracte basat. - Identificar, planificar, prioritzar i revisar les activitat amb impacte transversal.	
Entrades	**Sortides**
- Informes i quadres de comandament de seguiment - Actes comitè operatiu contracte basat - Decisions a prendre	- Acta (signada entre les parts) - Decisions preses - Propostes pel comitè estratègic de l'AM - Propostes per l'Òrgan de Contractació mitjançant el comitè estratègic de l'AM
Periodicitat	
Trimestral o a petició de l'Agència	

El proveïdor assignarà un cap de serveis del contracte per cada basat.

Cap de serveis del contracte

Realitzarà funcions de direcció, planificació, supervisió i coordinació dels diferents caps d'equip/projecte. Vetllarà per la correcta coordinació dels serveis del contracte tot garantint-ne l'assoliment dels objectius. Garantirà que els equips del servei objecte del contracte siguin els més adequats per l'assoliment dels objectius.

4.5.3 Comitè Operatiu Contractes Basats

Per cada un dels contractes basats, i segons la configuracions dels serveis i projectes que en formin part, es realitzarà un o diversos comitès operatius. Els diferents contractes basats concretaran la configuració d'aquests comitès. La periodicitat d'aquest comitè es preveu que sigui mensual, però aquest termini es podrà modificar d'acord amb les especificitats i necessitats del servei.

Títol
Comitè Operatiu Contracte Basat
Participants

Agència	***Altres Proveïdors***	***Empresa Homologada***
- Responsables del servei - Responsable del Contracte Basat (si escau) - Altres assistents (si escau)	- Responsables operatius de serveis d'altres contractes relacionats amb el servei del basat (diferents basats del mateix Acord Marc o d'altres, si s'escau)	- Responsables operatius del servei - Cap de serveis del contracte (si escau)
Objectius		
- Realitzar el seguiment i control de l'operació i provisió dels serveis del contracte basat. - Fer el seguiment dels ANS del contracte basat. - Planificar, prioritzar i revisar les iniciatives en curs. - Identificar possibles millores detectades en el servei per escalar al comitè executiu. - Identificar possibles canvis detectades en el servei per escalar al comitè executiu. - Tractament de les problemàtiques específiques - Desenvolupar i mantenir els procediments operatius necessaris per al correcte funcionament del serveis. - Qualsevol altre seguiment operatiu específic del model de gestió del servei del contracte basat.		
Entrades	**Sortides**	
- Quadres de seguiment del servei i ANS - Anàlisi i propostes de millora - Incidències detectades - Decisions a prendre	- Acta - Propostes al comitè executiu del contracte basat - Informes i quadres de comandament de seguiment del servei que es determinin per la gestió del servei. - Nous procediments operatius - Decisions preses	
Periodicitat		
Quinzenal o a petició de l'Agència		

En aquest sentit, el proveïdor haurà d'incorporar als diferents comitès les persones responsables de cada àmbit d'execució en funció dels temes específics a tractar en el comitè.

4.6 Localització física i recursos necessaris

El servei es realitzarà a les dependències del proveïdor i en els edificis de la Generalitat on es presti el servei, així com les altres localitzacions que l'Agència de Ciberseguretat de Catalunya pugui especificar en les contractacions basades posteriors per assegurar el correcte compliment en l'exercici de les seves funcions.