Plec de prescripcions tècniques particulars que regeix l'acord marc per l'entrega de serveis de suport al subministrament de maquinari, programari, llicències i solucions i integració operativa per l'Agència de Ciberseguretat de la Generalitat de Catalunya.

Lot 1: Serveis de suport de subministrament d'eines associades a la Ciberseguretat

Lot 2: Serveis de suport al desplegament i integració operativa de solucions de seguretat

Lot 3: Serveis de suport d'anàlisi de solucions de Ciberseguretat amb innovació oberta

Exp. AM.05.2024

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, 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 avançades, 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 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 dü 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

En el marc del present plec tècnic per al subministrament maquinari, programari, llicències, productes i/o solucions i suports de fabricant de Ciberseguretat, així com el desplegament, instal·lació, i configuració de les solucions. I, addicionalment, serveis d'anàlisi de solucions amb innovació oberta, es busca establir un estàndard d'excel·lència en la protecció de la infraestructura digital. El proveïdor seleccionat haurà de proveir equips d'última generació, programes d'avantguarda, llicències actualitzades i el seu suport i assistència per garantir la integritat, confidencialitat i disponibilitat dels nostres actius digitals.

La implementació de solucions de ciberseguretat eficients és essencial per prevenir amenaces emergents i salvaguardar la informació sensible. Així mateix, s'espera que el proveïdor demostri experiència en la instal·lació i configuració d'aquests sistemes, garantint una integració sense inconvenients amb la infraestructura vigent.

L'objecte d'aquest acord és establir la base contractual que permeti a l'Agència l'execució i garantia de les polítiques públiques en matèria de ciberseguretat, mitjançant la corresponent l'adquisició i el desplegament de solucions de ciberseguretat.

Aquest acord marc s'estructura en aquests lots:

- **Lot 1:** Serveis de suport de subministrament d'eines associades a la ciberseguretat
- **Lot 2:** Serveis de suport al desplegament i integració operativa de solucions de seguretat
- **Lot 3:** Serveis de suport d'anàlisi de solucions de Ciberseguretat amb innovació oberta

Així, es defineixen les prescripcions tècniques particulars que han de regir les prestacions i qualitats dels subministraments i serveis inclosos en els lots corresponents, detallant el seu abast objectiu, així com els requisits mínims i condicions tècniques generals que es consideraran per a la conclusió dels seus contractes derivats. Al tractar-se d'un acord marc on els lots no tenen tots els seus termes establerts, seran els documents de licitació dels contractes derivats els que especificaran els requisits funcionals i/o tècnics dels productes i/o serveis a adquirir.

Lot 1: Serveis de suport de subministrament d'eines associades a la ciberseguretat

L'abast d'aquest lot inclou:

- Adquisició de maquinari, programari, llicències, productes i/o solucions i suports de fabricant especialitzat en ciberseguretat.
- Suport tècnic del fabricant per a l'evolució tecnològica de les solucions i la resolució d'incidències.
- Garantia i manteniment de les eines i productes adquirits.
- Assegurar la compatibilitat, interoperabilitat i la integrabilitat de les eines i productes subministrats amb les solucions de ciberseguretat ja implementades.
- Assistència professional del fabricant

Lot 2: Serveis de suport al desplegament i integració operativa de solucions de seguretat

L'abast d'aquest lot inclou:

- Serveis d'anàlisi i disseny, desplegament, instal·lació, configuració, generació de documentació i posada en producció de les solucions de Ciberseguretat adquirides.
- Integració efectiva de les solucions amb el Security Operations Center (SOC) de l'Agència i altres eines associades a la ciberseguretat.
- Suport tècnic de l'integrador per a resolució d'incidències, amb el recolzament del fabricant quan s'escaigui necessari, incloent, però no només, la garantia del correcte desplegament.

Lot 3: Serveis de suport d'anàlisi de solucions de Ciberseguretat amb innovació oberta

L'abast d'aquest lot inclou:

- Metodologies de recerca i d'anàlisis de mercat amb component innovadora.
- Fases d'estudi d'alternatives tecnològiques i de serveis.
- Generació de models, documentació estadística i presentació de resultats.
- Definició estratègica de compra en base als models seleccionats.
- Suport i acompanyament a la redacció de documents relacionats amb el procés de compra.

Elements bàsics d'execució

A banda de les funcions i tasques pròpies de cada Lot, els proveïdors adjudicataris hauran de desenvolupar tasques transversals i comunes a la resta de serveis de l'Agència, pel bon funcionament de l'organització.

Es relacionen a continuació un seguit de tasques comunes en tots els lots i de caràcter transversal a la resta de serveis de l'Agència de Ciberseguretat per al bon funcionament de l'organització.

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.
- Mantenir actualitzada 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.
- Participar en el model de relació amb els clients de l'Agència, involucrant-se amb ells segons les necessitats de seguretat, el reporting requerit i les tipologies d'activitat.
- Participar 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.

- Gestionar 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.
- Realitzar el pla d'actuació periòdic amb les tasques planificades per les diferents iniciatives d'evolució o transformació per la pròpia operació del servei.
- Definir i gestionar el pla de capacitat del servei, així com la resta de tasques assignades a les funcions de servei.
- Gestionar 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.
- Definició, creació, distribució i manteniment dels informes del servei i de risc derivats de l'activitat.
- Realitzar anàlisis i proves de les eines que es considerin oportunes per a la millora o industrialització del servei.
- Proposar 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

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,..), així com adequar-se a noves necessitats i tecnologies que puguin esdevenir del propi procés d'innovació o transformació dels serveis.

2.1 LOT 1: Serveis de suport de subministrament d'eines associades a la ciberseguretat

Podran ser objecte de les licitacions per a l'adjudicació dels contractes derivats d'aquest lot, el subministrament de maquinari, programari, llicències, productes i/o solucions i

suports de fabricant que es puguin adquirir de forma independent als equipaments de referència que presten serveis a l'Agència.

Sens perjudici de les categories que s'exposen a continuació, que es detallen als efectes de que les empreses homologades coneguin l'abast de les eines i productes que es poden demanar, s'informa que en el Plec de Clàusules Administratives es detalla l'estratègia d'adjudicació d'aquests elements, que es centra en la separació per blocs de volum de necessitat. A aquests efectes, en l'annex 2 del PCAP es detallen els blocs mencionats.

3.11.1. Eines i productes

En aquest apartat es descriuen de forma general les eines i productes que l'Agència demanarà a les empreses homologades. En aquest sentit, la evolució de la tecnologia ha generat una diversificació d'entorns que van més enllà del físic i del virtual o cloud.

En aquest context, és essencial que els productes destinats a satisfer les demandes de l'Agència siguin versàtils i capaces d'abastar una àmplia gamma d'entorns tecnològics. Per tant, es demanarà maquinari, programari, llicències, productes i/o solucions i suport de fabricant per a tot tipus de dispositius i entorns com, per exemple: IoT (Internt of Things), OT (Operational Technology), IT (Information Technology) i IoMT (Internet of Medical Things) entre altres.

Aquestes eines i productes permetran realitzar de forma automatitzada, entre altres coses, el monitoratge i la detecció d'ameneces, identificar patrons d'atac i dispositius compromesos, així com la possible recuperació automatitzada de dades sensibles filtrades.

Donada la diversitat d'entorns tecnològics i de dispositius, la capacitat d'integració i interoperabilitat de les eines i productes que seran subministrats esdevé un criteri essencial.

3.11.1.1. Eines i productes de Control d'accés

Una entitat pública consta de diferents perfils d'usuari i cada usuari té unes credencials d'accés personalitzades, unides a unes polítiques de seguretat adequades per a cada tipus d'usuari, permeten controlar l'accés als recursos disponibles. Inclou totes les eines i productes que faciliten aquestes capacitats:

- Administra i controla l'accés d'un conjunt d'usuaris i dispositius a una xarxa amb solucions de seguretat específiques.
- Permeten l'autenticació mitjançant atributs físics únics com la petjada dactilar o l'iris de l'ull.
- Habiliten l'accés a múltiples sistemes amb una única autenticació, eliminant la necessitat de repetir el procés per a cada servei.
- Verifiquen la identitat d'usuaris o dispositius en una arquitectura de xarxa protegida, assegurant que només les identitats autoritzades accedeixin als serveis d'una organització.

- Capacitat d'autenticació robusta o multifactor per evitar atacs de força bruta, com per exemple les claus d'accés d'un sol ús (tokens).
- Permet l'accés segur als actius crítics gestionant i monitoritzant comptes privilegiats i accessos, protegint credencials i controlant l'accés a comptes privilegiats.
- Proporciona serveis centralitzats i sincronitzats d'identitats digitals, generant identitats úniques per a cada usuari i associant atributs per autenticació i autorització.

3.11.1.2. Eines i productes d'operació de la seguretat

Comprèn les capacitat que faciliten la gestió de la seguretat durant l'explotació d'un sistema informàtic, des de la implantació i la posada en funcionament fins al final del servei, permetent mantenir una correcta configuració de les mesures de protecció i els nivells de seguretat en el seu dia a dia. Inclou totes les eines i productes que faciliten aquestes capacitats:

- Prevenció, detecció i desinfecció de virus informàtics amb productes avançats per mantenir la seguretat del sistema.
- Detecta i bloqueja codi maliciós desconegut amb funcionalitats de monitorització, observació d'execució de processos i característiques Incident Response.
- Gestionen centralitzadament la infraestructura de dispositius en una xarxa, monitoritzant el rendiment i consum de recursos i resolent problemes de xarxa.
- Actualitzen components programari per corregir errors de seguretat, vulnerabilitats i afegir noves funcionalitats als sistemes.
- Protegeixen l'usuari durant la navegació per Internet controlant l'accés a llocs web basant-se en llistes de confiança o reputació.
- Suporta la monitorització de la seguretat recopilant, analitzant i confrontant informació sobre esdeveniments de seguretat i anomalies, facilitant la detecció i notificació d'incidents.
- Controla i salvaguarda les claus criptogràfiques durant tot el seu cicle de vida per a la protecció de comunicacions i informació emmagatzemada.
- Gestionen eficientment la diversitat i el desplegament massiu de dispositius en una organització, aplicant polítiques de seguretat i configuracions.

- Gestionen incidents, automatitzen tasques, coordinen respostes i ofereixen capacitats de correlació i processament d'alertes per millorar la detecció i resposta als incidents de seguretat.

3.11.1.3. Eines i productes de Monitorització de la seguretat

La reacció efectiva davant incidents de seguretat es fonamenta en la ràpida detecció i correcta identificació d'activitats que suggereixin un compromís en els sistemes. Això involucra l'ús de productes que possibiliten el monitoratge continu de la seguretat mitjançant l'automatització de l'anàlisi d'esdeveniments de seguretat, la recopilació i notificació d'informació pertinent, així com la potencial reacció enfront dels incidents detectats. Inclou totes les eines i productes que faciliten aquestes capacitats:

- Detecten i eviten accessos no autoritzats mitjançant el monitoratge del trànsit de xarxa per prevenir comportaments sospitosos.
- Atrauen i detecten activitats malicioses en una xarxa o aplicació simulada que emula sistemes d'interès per a un atacant, permetent el monitoratge per millorar els mecanismes de protecció de les xarxes reals de l'organització.
- Recopilen, mostren i analitzen el trànsit d'una xarxa per facilitar la detecció i investigació de possibles esdeveniments de seguretat, especialment relacionats amb l'ús no adequat o no autoritzat de protocols de xarxa.
- Executen aplicacions de manera aïllada i controlada per analitzar la seva execució i detectar la presència de codi maliciós. Garanteixen que, en cas de contenir malware, el sistema on es desplega l'eina de sandbox no s'infecti.

3.11.1.4. Eines i productes de Protecció de les comunicacions

Engloba eines i productes el propòsit principal dels quals és el de la protecció de les comunicacions establertes entre sistemes i/o dispositius connectats dins d'una xarxa i dispositius mòbils. Entre les seves funcions principals són establir un perímetre de seguretat, garantir comunicacions segures i prevenir atacs provinents d'altres xarxes externes. Inclou totes les eines i productes que faciliten aquestes capacitats:

- Controlen els fluxos d'informació entre xarxes, bloquejant accessos no autoritzats i evitant la propagació de programari maliciós.
- Actuen com a intermediaris en comunicacions entre xarxes internes i externes, mascarant l'usuari davant possibles atacants.
- Permeten la interconnexió de xarxes evitant filtracions d'informació no autoritzada en ambdues direccions.

- Limiten la connectivitat entre equips/xarxes, permetent el flux d'informació en un únic sentit i evitant la comunicació en la direcció oposada.
- Destinades al xifrat de canals de comunicació per preservar la confidencialitat i integritat de la informació.
- Analitzen i filtren el trànsit dirigit a aplicacions web específiques, oferint protecció a la Capa d'Aplicació del model OSI.
- Tecnologia que centralitza la lògica de control de les xarxes, permet desenvolupar aplicacions per programar-les i automatitza els processos operatius, separant físicament el pla de dades i control.
- Proporcionar un robust xifrat d'extrem a extrem per protegir la confidencialitat de la informació transmesa en la comuncició de dispositius mòbils, i integrar funcionalitats avançades de detecció i prevenció d'amenaces, com ara l'anàlisi de trànsit maliciós i la identificació de possibles vulnerabilitats.
- En dispositius mòbils assegurar la integritat de les claus xifrat, per garantir que només els usuaris autoritzats tinguis accés i evitint possibles vulnerabilitats.
- Autentificació multifactor per a dispositius mòbils per enfortir la seguretat mitjançant la verificació de la identitat de l'usuari a través de múltiples factors, afegint capes de protecció addicional.

3.11.1.5. Eines i productes de Protecció a la informació i suports d'informació

Engloba les eines i productes amb l'objectiu de reforçar les mesures de protecció de la informació, així com d'aquells suports que utilitzi, per tal d'assegurar alguna (o totes) les dimensions de seguretat incloent-hi la seva disponibilitat, integritat i confidencialitat, així com el no repudi de la informació. Inclou totes les eines i productes que faciliten aquestes capacitats:

- Destinat al xifrat i desxifrat d'arxius i dispositius d'emmagatzematge per protegir la confidencialitat i permetre l'accés només a usuaris autoritzats.
- Eines que faciliten l'intercanvi segur d'informació o arxius mitjançant el xifrat.
- Permeten eliminar informació electrònica de forma segura, fent que els continguts eliminats siguin irrecuperables.
- Productes de control de continguts (DLP) que impedeixen la transferència no autoritzada i la fuga d'informació altament confidencial. Controlen l'accés físic a ports i dispositius extraïbles.

- Inclouen dispositius i eines per a sistemes de signatura electrònica, permetent la generació i validació de signatures digitals per salvaguardar la confidencialitat, integritat i no repudi de la informació signada.
- Dispositius criptogràfics basats en maquinari que generen, emmagatzemen i protegeixen claus criptogràfiques, sovint proporcionant acceleració de maquinari per a operacions criptogràfiques.
- Comprèn eines que gestionen les metadates d'arxius, com documents d'oficina o arxius multimèdia, segons la política establerta en una organització.
- Eines de ciberseguretat capaces de recopilar, processar i analitzar grans volums de dades relacionades amb la seguretat de sistemes, xarxes i informació en general. Inclouen programari per a adquisició de dades, anàlisi d'evidència digital, monitoratge i detecció d'amenaces, xifrat i protecció de dades, anàlisi de vulnerabilitats i intel·ligència artificial per a identificació, prevenció i resposta a possibles atacs cibernètics.

3.11.1.6. Eines i productes de Protecció d'equips i serveis

La seguretat en les TIC recau en gran mesura en la protecció correcta dels equips sobre els quals es processa la informació, així com dels serveis que s'hi executen. Inclou totes les eines i productes que faciliten aquestes capacitats:

- Analitzen el flux de correus electrònics per evitar que aquells considerats nocius arribin als usuaris finals. Busquen paraules i patrons sospitosos en el contingut dels missatges per filtrar-los o etiquetar-los i evitar que arribin a la safata d'entrada.
- Permeten l'execució de lògica programada en els seus circuits integrats per a diversos fins, alhora que proporcionen interfícies per a la comunicació amb els sistemes amb els quals han d'interactuar. Poden estar equipades amb diferents mecanismes de protecció per salvaguardar les dades que contenen o les dades intercanviades per dur a terme la seva funcionalitat.
- Productes o sistemes que serveixen com a base o suport per a l'execució de determinats mòduls de programari.
- Ofereixen visibilitat i control sobre l'ús que fan els usuaris d'una organització d'aplicacions i serveis al núvol. Representen un punt central on l'organització pot implementar polítiques de seguretat per regular l'ús d'aplicacions i serveis al núvol.

- Responen a la necessitat d'establir mecanismes d'autenticació i identificació remota per reduir els desplaçaments dels ciutadans per realitzar tràmits. Realitzen comparacions entre una persona i la foto del document d'identitat i implementen controls de seguretat en temps real, com la detecció d'hologrames, distintius, patrons i altres elements de seguretat del document d'identitat.
- Permetin la simulació d'atacs i de qualsevol operació de l'àmbit de la ciberseguretat.

3.11.1.7. Eines i productes pels serveis de conformitat i governança de la seguretat

Eines i solucions que defineix com a productes de Conformitat i Governança de la Seguretat tals com aquells que faciliten desenvolupar activitats en els següents àmbits:

- Governança i la planificació pròpia de la seguretat
- Compliment de la normativa de seguretat i conformitat
- Anàlisi i gestió de riscos
- Notificació i gestió de ciberincidents
- Identificació i intercanvi de ciberintel·ligència
- Formació i conscienciació en ciberseguretat.

Inclou totes les eines i productes que faciliten aquestes capacitats:

- Solucions que assisteixen als usuaris en obtenir informació sobre l'estat de seguretat dels sistemes dels organismes, basant-se en estàndards de mesurament. Proporcionen índexs per avaluar les dades, interpretar-les i prendre decisions estratègiques. Poden facilitar l'elaboració de Plans d'Adequació i mesures tècniques per aplicar a sistemes.
- Solucions que ajuden als usuaris en la preparació d'auditories, gestió del compliment i certificacions, i gestió de la seguretat del sistema. Proporcionen assistència als auditors amb capacitats de recopilació automàtica d'evidències, llistes de comprovació i quaderns d'auditoria, automatització de l'anàlisi del compliment, generació d'indicadors i d'informes de compliment i altres tasques necessàries a les diferents fases de l'auditoria. També inclou eines i productes que faciliten l'anàlisi i el monitoratge continu del compliment de la normativa de Ciberseguretat.
- Solucions que ajuden als usuaris a realitzar l'Anàlisi de Riscos associada als sistemes. Identifiquen amenaces als actius essencials del sistema i

analitzen la probabilitat i l'impacte de la materialització. Oferixen la possibilitat de mitigar o reduir els riscos a través de salvaguardes.

- Solucions que automatitzen processos, classifiquen incidents, faciliten el seguiment de la gestió i permeten la coordinació entre els diferents actors implicats. Poden ajudar tant als operadors que gestionen incidents com als usuaris que notifiquen incidents de seguretat.
- Solucions destinades a la gestió i intercanvi de ciberintel·ligència, millorant les capacitats de prevenció, anàlisi i detecció de ciberamenaces.
- Solucions dedicades a avaluar, capacitar, reforçar i mesurar els nivells de formació i conscienciació en ciberseguretat dels empleats d'un organisme.

3.11.1.8. Eines d'intel·ligència artificial

Seran totes aquelles eines que suportin les activitats de ciberseguretat a través d'algoritmes avançats i d'intel·ligència artificial, d'acord amb les premisses establertes per l'Esquema Nacional de Ciberseguretat o aquelles a les que l'Agència de Ciberseguretat de Catalunya estableixi en cada moment.

3.11.1.9. Eines i productes d'anàlisi forense

Eines i productes d'anàlisi forense en ciberseguretat per la investigació i resposta a incidents, proporcionant les capacitats necessàries per identificar, analitzar i mitigar amenaces cibernètiques. Inclou totes les eines i productes que faciliten aquestes capacitats:

- Recopilació i preservació forense de dades per facilitar la recol·lecció i conservació de dades digitals per permetre la reconstrucció precisa d'esdeveniments.
- Recerca i anàlisi eficient per oferir funcionalitats avançades per examinar grans volums de dades, identificant patrons, anomalies i evidències digitals rellevants de manera efectiva.
- Generació d'informes detallats que permetin la creació d'informes exhaustius i cronologies d'esdeveniments, facilitant la comprensió i comunicació dels detalls clau en la recerca forense.
- Traçabilitat d'activitats malicioses que ajudin en la identificació i seguiment d'accions malicioses, proporcionant una visió clara de la cadena d'esdeveniments en un incident de ciberseguretat.
- Dissenyades per preservar la integritat de l'evidència digital, assegurant la seva validesa i admissibilitat en procediments legals.

3.11.1.10. Eines i productes amb capacitats de recuperació

Les eines i productes destinats a la gestió de còpies de seguretat per la preservació i recuperació de dades en entorns digitals. Aquestes solucions ofereixen una varietat de capacitats, des de la programació automatitzada de còpies de seguretat fins a la gestió eficient de grans volums de dades. Inclou totes les eines i productes que faciliten aquestes capacitats:

- Programació automatitzada de còpies de seguretat permeten establir programacions automàtiques per a la realització periòdica de còpies de seguretat, assegurant l'actualització constant de la informació.
- Oferir capacitats per gestionar de manera eficient grans quantitats d'informació, garantint la integritat i disponibilitat de les dades recolzades.
- Optimitza l'espai d'emmagatzematge mitjançant la implementació de tecnologies avançades, com deduplicació i compressió, per maximitzar l'eficiència en el resguard de dades.
- Proporcionar la capacitat de restaurar dades de manera ràpida i fiable, facilitant la recuperació eficient en situacions de pèrdua o corrupció d'informació.
- Incorporar funcionalitats de xifrat per garantir la seguretat de les dades emmagatzemades, protegint la confidencialitat de la informació recolzada.
- Aplicar les polítiques de còpies de seguretat definides per l'organització, facilitant còpies de seguretat de sistemes d'emmagatzematge, equips o sistemes complets.
- Inmutabilitat, integritat, robustesa i confiabilitat de la informació i de les dades en les còpies realitzades.

3.11.1.11. Altres eines i productes

Recull d'eines i productes on la funcionalitat principal de seguretat, per la seva naturalesa específica, no s'enquadra dins de cap altra de les categories especificades en anterioritat.

Alguns exemples podrien ser:

- Eines i productes pel desenvolupament de productes de ciberseguretat.
- Eines i productes pel descobriment i governança de dades i actius en les xarxes.
- Altres.

3.11.2. Subministraments i suport del fabricant

Els adjudicataris hauran de ser capaços de subministrar els productes que compleixin les prescripcions de les licitacions dels contractes derivats, on estaran definits els requeriments tècnics i funcionals. De forma general, un subministrament inclourà l'adquisició, emmagatzematge i lliurament dels productes i l'activació dels manteniments i suports de fabricant d'aquests, un cop posats en producció.

3.11.3. Servei d'assistència professional del fabricant

Per optimitzar l'ús d'eines i productes, és fonamental comptar amb una assistència i assessorament continu proporcionats pel fabricant. Aquestes funcions no només asseguren una resposta ràpida en assessorament en necessitats tècniques, sinó que també facilita un accés continu a assessorament especialitzat per aprofitar al màxim les capacitats de les eines. Aquest enfocament proactiu contribueix a l'eficàcia operativa i millorar la competència en l'ús de les eines, convertint-se així en un recurs valuós per maximitzar l'eficiència i el rendiment de les solucions proporcionades pel fabricant.

3.11.4. Evolució, desenvolupament i innovació

Durant la execució i durada dels diferents basats ens podem trobar que l'evolució i desenvolupament d'eines de seguretat és un procés continu i dinàmic. A mesura que les amenaces cibernètiques evolucionen, les eines de seguretat han d'adaptar-se i millorar per protegir la integritat, confidencialitat i disponibilitat de la informació.

L'evolució de les eines de seguretat és contínua, ja que els desafiaments de seguretat cibernètica continuen canviant i presentant noves amenaces. La combinació de múltiples capes de seguretat i enfocaments proactius serà essencial per fer front a un panorama d'amenaces en constant canvi.

Es podrà sol·licitar a les empreses homologades que aportin el seu coneixement per evolucionar, innovar, identificar noves necessitats i millorar de qualsevol dels aspectes relacionats en la prestació de serveis associats en aquest lot de l'Acord Marc, tot aportant metodologies contrastades basades en la innovació.

3.11.5. Assegurar la compatibilitat i integració amb les solucions de ciberseguretat

Garantir la compatibilitat i integració efectiva amb les solucions de ciberseguretat implementades és una prioritat fonamental en l'adopció de les eines, programari i llicències subministrades. El licitador s'ha de comprometre a realitzar una exhaustiva avaluació de la infraestructura existent, assegurant-nos que les noves addicions siguin perfectament alineades amb els sistemes de seguretat preexistents.

El nostre enfocament se centra en la interoperabilitat, evitant possibles conflictes i optimitzant l'eficiència operativa. A més, s'han de comprometre a treballar estretament amb l'equip de seguretat de la Agència per integrar de manera transparent les noves solucions, maximitzant així la capacitat de defensa contra amenaces cibernètiques. La compatibilitat no es limitarà només als aspectes tècnics, sinó que també considerarà la coherència en les polítiques de seguretat, proporcionant una estratègia integral que enforteixi la postura general de ciberseguretat de la Agència. Aquest compromís busca no només proporcionar eines efectives, programari i llicències, sinó també garantir la seva harmoniosa integració per oferir una defensa sòlida i coordinada contra les creixents amenaces digitals.

3.11.6. Condicions específiques d'inici d'activació de les llicències

Tots aquells tipus de llicenciaments associats a desplegaments, instal·lacions, configuracions i/o integracions s'activaran en el moment de la posada en producció de la solució. Tot coincidint amb l'acceptació i conformitat per part de l'Agència de totes les evidències de qualitat d'entrega i certificats de fabricant que puguin ser requerits.

Per tant, l'activació de les llicències coincidirà en el moment en que l'Agència comença a consumir els serveis, solucions i/o productes subministrats.

Rols i funcions del Lot

A títol enunciatiu i no limitatiu es defineixen els rols i les funcions que es podran sol·licitar en els posteriors contractes basats d'aquest lot de manera no acumulativa. Un mateix perfil podrà assumir més d'un rol/funció:

Nom Capacitat	Funcions
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. També serà l'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. Realitzarà funcions de direcció global. Vetllarà per la correcta coordinació dels serveis i projectes dels contractes basats, tot garantint-ne l'assoliment dels objectius. Garantirà que els equips de gestió siguin els més adequats per l'assoliment dels objectius. També participarà en els òrgans de govern del contracte d'acord amb el Model de Relació. Aquesta figura ha d'estar durant tota la durada de l'Acord Marc. Aquesta figura és obligatòria per a qualsevol empresa que s'homologui i serà comuna als eventuals contactes basats que puguin adjudicar-se a casa companyia.
Coordinador	Lideratge del basat, planificació, supervisió i coordinació dels diferents perfils implicats en la prestació de serveis del contracte. Actuar com a enllaç entre el proveïdor i els diferents agents i fabricants implicats en l'ecosistema de l'Agència. En funció del contracte basat que es tracti aquest podrà coincidir amb el responsable de l'empresa homologada.

2.2 LOT 2: Serveis de suport al desplegament i integració operativa de solucions de seguretat

Es sol·licitarà a les empreses els serveis per desplegar i/o integrar les noves eines adquirides per l'Agència. Segons l'eina o producte a instal·lar, o a integrar, es podran donar diverses casuístiques. És per aquest motiu, que les empreses hauran de presentar les capacitats necessàries per participar en qualsevol de les fases que a continuació es detallen:

- Gestió global del servei
- Anàlisi i disseny
- Pilots, implantació i integració
- Entrega, suport i acompanyament
- Innovació i evolució

Aquest servei precisa d'un enfoc metodològic tal que garanteixi els objectius que es plantegin en cadascuna de les fases anteriors. A continuació es detallen les fases per les quals es podran sol·licitar els serveis d'implantació i integració.

3.11.7. Gestió global del servei

Es sol·licitarà, en aquest cas, que el servei disposi d'una capa de gestió que asseguri la qualitat de les tasques a realitzar mitjançant el control i seguiment d'aquestes i el reporting en els diferents nivells decisors i als diferents involucrats en el projecte. A més, a més, el servei haurà de ser capaç d'adaptar-se als diferents nivells d'interlocució, així com de gestionar el seu propi equip i el servei extrem a extrem. Aquesta gestió global del servei haurà d'incloure, com a mínim, els següents punts:

Gestió global del servei:algunes d'aquestes tasques seran:

  - Coordinar a totes les parts involucrades i trobar sinèrgies.
  - Suport, col·laboració i coordinació amb els proveïdors i terceres empreses de l'ecosistema de l'Agència.
  - Reportar, informar i/o comunicar sobre l'estat de les iniciatives en curs, i riscos detectats.
  - Abordar les iniciatives d'innovació i de millora contínua i validar i consolidar la qualitat i continuïtat en els nous serveis i millores implantades.

- **Implantació del model organitzatiu de l'equip del servei:** establir quin serà el model d'organització associat a l'equip adscrit al contracte.
- **Gestió dels recursos assignats al servei**: caldrà una correcta assignació de les persones al projecte, així com els seus rols i funcions.
- **Reportar i generar informes:** s'hauran de generar tots els reports i informes adients per a la correcta execució de cadascuna de les fases del projecte, informant sobre l'estat de situació, avanços i riscos, sobre els quals caldrà fer una valoració adequada per tal d'assegurar la continuïtat del servei. Els informes hauran d'estar

preparats ad-hoc per a cada nivell i àmbit d'interlocució. Es preveuen reports que s'hauran de generar de forma periòdica i, d'altres de forma puntual o sota demanda.

- **Gestió econòmica i pressupostària del servei:** caldrà realitzar un seguiment econòmic i pressupostari exhaustiu de l'execució del servei.
- **Gestió i seguiment de la planificació i de l'abast del servei:** el licitador haurà de presentar i consensuar la planificació de cadascuna de les fases del projecte, indicant quin serà el seguiment del seu abast de manera que es pugui controlar i seguir les necessitats funcionals i tècniques de la implantació.
- **Gestió i seguiment dels riscos i implantar accions mitigadores:** el licitador haurà de presentar per cadascun dels riscos identificats en els informes de reporting les accions mitigadores, correctives i de contingència que assegurin la continuïtat del projecte.
- **Responsabilitat i interlocució amb l'Agència:** l'empresa s'haurà de fer càrrec extrem a extrem del servei i, per tant, es sol·licita que la responsabilitat d'aquesta gestió estigui sota un Service Manager, el qual serà el seu principal punt de contacte per a l'Agència.

3.11.8. Anàlisi i disseny

Es podrà sol·licitar els serveis d'anàlisi i disseny d'una solució tecnològica de l'àmbit de la seguretat per tal que.

3.11.8.1. Anàlisi de requisits tècnics i funcionals

En aquest cas, es sol·licitarà que l'empresa faci un anàlisi detallat dels entorns específics de ciberseguretat, així com qualsevol altre aspecte relacionat que pugui considerar-se rellevant.

L'objectiu serà transformar les necessitats en requisits tècnics i funcionals del futur escenari. Sense ser exhaustius, serà d'especial importància l'anàlisi de:

- Volumetries, estats i capacitats els sistemes sota estudi.
- Anàlisi respecte a capacitats d'escalabilitat i evolució.
- Recavar informació per facilitar el dimensionament futur.
- Anàlisi de requeriments tècnics i funcionals d'alt i baix nivell.
- Anàlisi de solucions de mercat amb anàlisis comparatiu de productes, equips, requeriments tècnics i funcionals, previsions d'evolució tecnològica...
- Matriu d'encreuament d'indicadors i dimensions dels anàlisis efectuats.
- Identificació de les fonts origen d'informació i del seu format.
- Identificació de possibles processos de càrrega d'informació.
- Identificar les diferents visualitzacions d'informes i quadres de comanament.
- Comprendre els controls de qualitat i de verificació actuals.
- Identificar altres aspectes tècnics-funcionals rellevants pel bon desenvolupament del projecte i possibles millores transversals a dur a terme.
- Aportar intel·ligència sectorial i el seu know-how sobre el mercat.

3.11.8.2. Disseny tècnic i funcional de la solució

Es podran sol·licitar serveis de disseny, tècnics i funcionals, d'una futura solució de ciberseguretat a un nivell de detall elevat, d'arquitectura general (High Level Design – HLD), i a un nivell de detall de baix nivell (Low Level Design – LLD). L'output d'aquests serveis hauran de ser uns lliurables clars i ordenats, amb tota mena de detalls i que segueixin una metodologia de treball constrastada.

Així doncs, i sense ser exhaustius, el disseny s'haurà de plantejar atenent criteris considerats clau en aquest àmbit, entre ells:

- **Fiabilitat, disponibilitat i capacitat de recuperació**: Garantir la màxima disponibilitat davant de caigudes d'enllaços o elements individuals, gestionant de manera eficaç les fallades que puguin afectar a la disponibilitat de la solució. S'ha d'assegurar la minimització en els temps de parada tant planificats com imprevistos mitjançant l'aplicació de les tècniques i els procediments adequats.
- **Flexibilitat**: Ser capaç d'adaptar-se als canvis evolutius que siguin necessaris per complir els requeriments tècnics i demanda prevista.
- **Escalabilitat**: Haurà de garantir la fàcil implementació de noves funcionalitats i serveis, així com donar resposta al creixement de la demanda a través d'un dimensionament correcte de recursos.
- **Seguretat i aïllament**: Incloure com a imprescindibles consideracions relatives a la seguretat, emprant les mesures de privacitat i confiabilitat que siguin d'aplicabilitat.

3.11.9. Pilots, implantació i integració

Es podrà sol·licitar els serveis de pilots, d'implantacions i d'integracions d'una solució.

3.11.9.1. Pilots i proves de concepte

Es sol·licitarà que l'empresa plantegi una proposta de Pla de Pilots i/o Proves de concepte PoC/MoC que es considerin més rellevants, amb la finalitat d'assegurar la idoneïtat d'una solució i que la implementació futura estigui adaptada a la solució desitjada.

Per això, les empreses hauran de contemplar, sense ser limitant ni exhaustiu, els aspectes següents:

- Selecció i priorització de pilots i proves de concepte que es considerin més rellevant, seleccionant els candidats a desenvolupar dins un pla de pilots i proves en entorns reals i productius.
- Presentació de la solució de disseny associada als pilots i proves, així com l'elaboració dels seus dissenys Low Level Design (LLD) com de High Level Design (HLD).
- Implantar la solució en un entorn productiu i real, encara que implantat en una selecció reduïda d'usuaris o clients.
- Presentació d'estudi en què es validi, de manera rigorosa, la viabilitat de la implantació en entorn real de la solució, així com les integracions que corresponguin amb tercers sistemes o elements, verificant els aspectes clau, tècnics i funcionals de la solució.
- S'haurà de seguir els estàndards i normatives pertinents.

Alguns dels lliurables associats a aquesta fase, sense ser exhaustiu ni limitant, podran ser els següents:

- Pla de pilots i proves
- Planificació detallada i calendari d'actuacions
- Disseny de la solució (LLD i HLD)
- Pla de validació i qualitat dels pilots i les proves
- Pla de reporting
- Lliurables parcials
- Informes finals amb els resultats dels pilots i les proves

3.11.9.2. Serveis d'implantació

Es podrà sol·licitar que l'empresa plantegi, de manera general, les que serien les fases d'execució de la implantació global de la solució.

Aquest plantejament haurà d'estar clarament definit per fases, ser coherent des del punt de vista d'enginyeria de processos i de metodologia de projectes.

Es podrà sol·licitar a l'empresa que inclogui detall de totes aquelles fases i subfases i/o subactivitats que consideri necessàries a la planificació associada.

L'empresa serà responsable de la implantació configuració i instal·lació total dels elements associats a la ciberseguretat (maquinari, programari, llicències...), tot seguint la planificació acordada.

L'empresa haurà de proveir els plans de proves unitàries pertinents per tal de validar que les solucions implementades compleixen amb els requisits definits. S'haurà de proporcionar assistència als usuaris en la comprovació de que les solucions implantades compleixen amb els requisits establerts.

3.11.9.3. Capacitat d'integració amb altres sistemes

A continuació, sense ser exhaustius, es llisten alguns possibles sistemes amb els quals les solucions es podran d'integrar i que es podrà sol·licitar a l'empresa:

- SIEM
- SOAR
- Datalake
- Eines transversals de gestió com, per exemple: ITSM Remedy per gestionar els tickets IT, Clarify per gestionar la facturació...
- Altres elements associats a la ciberseguretat

3.11.9.4. Integració efectiva amb el Security Operations Center (SOC) de l'Agència

La garantia d'integració efectiva del maquinari, programari, llicències, productes i/o solucions amb el Security Operations Center (SOC) de l'Agència és un compromís fonamental que adquiriran les empreses homologades en qualsevol dels serveis

encarregats. S'hauran d'assegurar que cada component proporcionat sigui perfectament compatible amb les infraestructures i processos existents al SOC, facilitant així una col·laboració íntegra i transparent. S'implementaran mesures específiques en cada cas per assegurar la interoperabilitat i la comunicació fluida entre les solucions subministrades i l'entorn del SOC. Això inclourà, entre d'altres, la configuració precisa de protocols de comunicació, la sincronització d'esdeveniments i la provisió d'interfícies eficients per al monitoratge i la gestió centralitzada.

L'activitat d'integració s'orientarà a enfortir la capacitat del SOC per detectar, analitzar i respondre a amenaces cibernètiques de manera proactiva.

3.11.10. Entrega, suport i acompanyament

Es podrà sol·licitar que l'empresa presenti i executi un pla d'entrega de la solució implantada als equips pertinents de l'Agència. Aquest pla, acordat entre totes les parts implicades a l'inici del servei, pot contenir, sense ser exhaustiu ni limitatiu, els següents apartats:

- Acompanyament als equips de l'Agència a la gestió del canvi
- Proves de qualificació i certificació
- Suport a la comunicació
- Formació i suport als agents i equips identificats
- Altra documentació associada

Qualitat i certificació a l'entrega

Per tal d'assegurar la implemtanció i/o integració de les solucions l'Agència podrà requerir, per a la seva conformitat, que l'empresa presenti proves i/o evidències que corrobori que les actuacions realitzats han estat satisfactòries com, per exemple:

- Certificacions del fabricant
- Adjunts i documents amb els tests de proves realitzats segons criteris establerts
- Altres tipus d'evidències

3.11.11. Serveis d'innovació i evolució

Es preveuen possibles evolucions de certes eines associades amb la ciberseguretat, per tal d'adaptar-se a les noves formes de treball i requeriments envers la ciberseguretat i normatives. Es podrà sol·licitar a les empreses que aportin el seu coneixement per evolucionar, innovar, identificar noves necessitats i millorar de qualsevol dels aspectes relacionats en la prestació de serveis associats en aquest Acord Marc, tot aportant metodologies contrastades basades en la innovació. Sense ser exhaustius, algunes de les activitats que les empreses hauran de dur a terme són:

- Suport a l'evolució de funcionalitats operatives i de processos de serveis.
- Suport als processos d'innovació en els serveis identificats a través de dinàmiques innovadores i metodologies de mercat com, per exemple, Design Thinking.

- Aportació de coneixement sobre les matèries a tractar, basat en l'experiència, el coneixement del mercat i de les tecnologies i en criteris objectius.
- Assegurar que en les implementacions, des de la fase inicial del projecte, el detall de la documentació i processos associats per tal que el pas a producció sigui directe i/o automàtic, facilitant el tancament administratiu dels projectes.
- Coordinació de totes les tasques amb tercers implicats, si s'escau.
- Proposar crear i/o modificar procediments i instruccions operatives en el cas que fos necessari, automatitzant les tasques integrades des de l'inici.
- Proposar, de forma proactiva i sistèmica, idees, oportunitats, reptes innovadors, PoCs, MoCs i projectes pilots relacionats amb la ciberseguretat.
- Donar suport als processos interns d'innovació i establir un model de relació adequat.
- Realitzar el seguiment dels processos d'innovació i avaluar els seus resultats.

3.11.12. Suport tècnic a través dels fabricants

El licitador ha de garantir que tot el maquinari, programari, llicències, productes i/o solucions subministrades siguin instal·lades i configurades. Per a aquestes activitats haurà de comptar amb el suport tècnic directe del fabricant, el qual haurà de saber fer-ne un ús adequat i pertinent. Aquest suport que oferiran els fabricants a l'empresa homologada, abastarà no només les implementacions o integracions, sinó també la resolució de possibles incidències, dubtes o altres qüestions esdevingudes.

Per tant, a les empreses homologades, segons s'estableixi en els contractes basats, se'ls hi podrà demanar el seu compromís a establir una col·laboració estreta amb els equips de suport tècnic dels fabricants corresponents, assegurant comptar amb recursos especialitzats per abordar qualsevol inconvenient de manera àgil i eficient.

A tal efecte, es podrà requerir el segell, certificació o garantia de fabricant en el desplegament i instal·lació dels seus productes. La prioritat és assegurar el correcte desplegament de la solució, optimitzant el seu rendiment i maximitzant la seva efectivitat en la protecció contra amenaces cibernètiques.

Rols i funcions del Lot

A títol enunciatiu i no limitatiu es defineixen els rols i les funcions que es podran sol·licitar en els posteriors contractes basats d'aquest lot de manera no acumulativa. Un mateix perfil podrà assumir més d'un rol/funció:

Nom Capacitat	Funcions
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. També serà l'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.

	Realitzarà funcions de direcció global. Vetllarà per la correcta coordinació dels serveis i projectes dels contractes basats, tot garantint-ne l'assoliment dels objectius. Garantirà que els equips de gestió siguin els més adequats per l'assoliment dels objectius. També participarà en els òrgans de govern del contracte d'acord amb el Model de Relació. Aquesta figura ha d'estar durant tota la durada de l'Acord Marc. Aquesta figura és obligatòria per a qualsevol empresa que s'homologui i serà comuna als eventuals contactes basats que puguin adjudicar-se a casa companyia.
Coordinador/ Cap de projecte	Lideratge del basat, planificació, supervisió i coordinació dels diferents perfils implicats en la prestació de serveis del contracte. Actuar com a enllaç entre el proveïdor i els diferents agents i fabricants implicats en l'ecosistema de l'Agència. Assegurar que tot el personal de l'adjudicatari que prestarà serveis, passi per un pla de conscienciació i formació en matèria de seguretat. Assegurar que tot el personal del proveïdor que hagi de tractar dades o sistemes de tractament de dades de nivell sensible o superior signin un Acord de Confidencialitat 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. Participar en el disseny fins a la implantació dels projectes de seguretat, incloent els aspectes de compliment normatiu, liderar plans de millora, elaborar informes d'activitat, dels serveis o projectes que li siguin encomanats, dintre dels marges de qualitat, temps i cost establerts, i marcant les directrius que l'equip ha de seguir per realitzar aquestes activitats. 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 En funció del contracte basat que es tracti aquest podrà coincidir amb el responsable de l'empresa homologada.
Arquitecte de seguretat	Encarregat de realitzar la presa de requeriments, donar les especificacions funcionals i dissenys tècnics necessaris.

	Responsable de l'anàlisi i el disseny conceptual de la solució i l'arquitectura de components tecnològics. Encarregat de definir i determinar la millor solució tècnica a nivell de seguretat, del dimensionament i configuració de la plataforma tecnològica.
Tècnic expert Ciberseguretat	Aquest especialista s'enfoca en la implementació i gestió de mesures de seguretat específiques per protegir els sistemes, xarxes i dades d'una organització contra amenaces cibernètiques. Sense ser exhaustius ni limitatius, entre les seves responsabilitats clau es descriuen les següents: • Configuració i administració d'eines de seguretat • Implementació de polítiques i procediments de Seguretat • Execució de pilots i proves de concepte, entre d'altres.

2.3 LOT 3: Serveis de suport d'anàlisi de solucions de Ciberseguretat amb innovació oberta

Es sol·licitarà a les empreses un servei que dongui suport als processos d'anàlisi de solucions amb caràcter intern. I, a més a més, que aquests processos estiguin dirigits i motivats amb metodologies contrastades de mercat, entre elles, metodologies basades en la innovació oberta.

Es podrà sol·licitar un servei extrem a extrem i serà autogestionat. Sense ser exhaustius ni limitatius, haurà d'estar basat, com a mínim, de les següents premises:

- Metodologies contrastades de mercat per a la gestió i govern del propi servei
- Metodologies de treball ben estructurades i definides basades en la innovació oberta.
- Mètodes d'anàlisi que permetin identificar l'estat de l'art, les necessitats i els reptes sota estudi.
- Estudis de les alternatives existents al mercat i en la realització de proves de concepte.
- Sistema de propostes que facilitin la selecció de models en base a recomanacions expertes.
- Suport i acompanyament a la definició estratègica de compra.
- Suport i acompanyament al procés de compra.

El servei haurà de contemplar tota la generació de lliurables i documents necessaris i acordats prèviament durant tota la durada del contracte basat.

Serà imprescindible que tot el procés d'anàlisi estigui guiat per empreses expertes en realitzar aquest tipus de serveis. I per tant es demanarà objectivitat i transparència. Tot indicant, si escau, aquells punts que puguin ser opinions o recomanacions expresses per part de l'empresa. I, en qualsevol cas, **per realitzar aquest servei es demanarà total independència de la tecnologia, marques, empreses tercers o productes.**

3.11.13. Metodologia de gestió i govern

Es sol·licitarà, en aquest cas, que el servei disposi d'una capa d'autogestió que asseguri la qualitat de les tasques a realitzar mitjançant el control, la coordinació i seguiment d'aquestes i el reporting en els diferents nivells decisors i als diferents involucrats en el projecte. A més, a més, el servei haurà de ser capaç d'adaptar-se als diferents nivells d'interlocució, així com de gestionar el seu propi equip i el servei extrem a extrem. Aquesta gestió global del servei haurà d'incloure, com a mínim, els següents punts:

- **Gestió global del servei:** algunes d'aquestes tasques seran:
  - Coordinar a totes les parts involucrades i trobar sinèrgies.
  - Reportar, informar i/o comunicar sobre l'estat de les iniciatives en curs, i riscos detectats.
  - Abordar les iniciatives d'innovació i de millora contínua i validar i consolidar la qualitat i continuïtat en els nous serveis i millores implantades.
- **Implantació del model organitzatiu de l'equip del servei:** establir quin serà el model d'organització associat a l'equip adscrit al contracte.
- **Gestió dels recursos assignats al servei**: caldrà una correcta assignació de les persones al projecte, així com els seus rols i funcions.
- **Reportar i generar informes:** s'hauran de generar tots els reports i informes adients per a la correcta execució de cadascuna de les fases del projecte, informant sobre l'estat de situació, avanços i riscos, sobre els quals caldrà fer una valoració adequada per tal d'assegurar la continuïtat del servei. Els informes hauran d'estar preparats ad-hoc per a cada nivell i àmbit d'interlocució. Es preveuen reports que s'hauran de generar de forma periòdica i, d'altres de forma puntual o sota demanda.
- **Gestió econòmica i pressupostària del servei:** caldrà realitzar un seguiment econòmic i pressupostari exhaustiu de l'execució del servei.
- **Gestió i seguiment de la planificació i de l'abast del servei:** el licitador haurà de presentar i consensuar la planificació de cadascuna de les fases del projecte, indicant quin serà el seguiment del seu abast de manera que es pugui controlar i seguir les necessitats funcionals i tècniques de la implantació.
- **Gestió i seguiment dels riscos i implantar accions mitigadores:** el licitador haurà de presentar per cadascun dels riscos identificats en els informes de reporting les accions mitigadores, correctives i de contingència que assegurin la continuïtat del projecte.
- **Gestió del servei i interlocució amb l'Agència:** l'empresa s'haurà de fer càrrec extrem a extrem del servei i, per tant, es sol·licita que la responsabilitat d'aquesta gestió estigui sota un Service Manager, el qual serà el seu principal punt de contacte.

Les empreses hauran de presentar la seva proposta metodològica en quant a la gestió, coordinació i govern d'aquest servei.

3.11.14. Metodologia de treball basada en la innovació oberta

Metodologies contrastades i certificades en serveis semblants, així com al inclusió de la component d'innovació oberta i la cocreació en el servei (design thinking...). Definició de les fases pròpies del servei.

3.11.14.1. Anàlisi de situació i de necessitats

Es demanarà métodes d'anàlisi, i la seva execució, que permetin identificat l'estat de l'art, la situació actual i les necessitats de l'Agència. Tan mateix, serà clau identificar els objectius aixçi com els criteris d'anàlisi de l'objecte en qüestió, expressat explícitament en el seu contracte basat de forma pertinent.

Entre les activitats i funcions que s'espera per part de les empreses homologades en aquest apartat, sense ser exhaustius ni limitants, seran les següents:

- Estructurar i dirigir entrevistes i tallers personals i/o grupals amb els stakeholders.
- Analitzar, estructurar i sintetitzar la documentació, volumetries i inventaris compartits.
- Recerca d'informació addicional en fonts alternatives.
- Suport i acompanyament a les consultes al mercat.

Identificar objectius i els criteris d'anàlisis i avaluació.

3.11.14.2. Estudi d'alternatives i proves de laboratori

Es demarà realitzar, sense ser exhaustius ni limitatius, les següents activitats:

- Prospeccions i estudis complexos de mercat
- Identificació de tendències tecnològiques i operatives
- Posicionar de forma comparativa i estructurada marques, productes, serveis, proveïdors... en les seves diferents vessants (econòmiques, operatives, tecnològiques...) que siguin d'interés i segueixin els criteris d'anàlisi i avaluació prèviament establerts.

Adicionalment, per tal de donar profunditat a l'anàlisi, i facilitar les futures decisions dels models identificats es podrà demanar les següents activitats relacionades amb proves i testejos:

- Identificació i definició de bancs de proves i sets de dades.
- Definició de criteris d'acceptació de les proves i objectius a assolir.
- Identificació de possibles candidats a fer proves i acompanyament al procés de formalització, desplegament... de les proves i testejos.
- Suport i acompanyament a la realització de proves de laboratis, demos, PoCs o pilots.

3.11.14.3. Selecció de models i recomanacions

En base a totes les premisses prèvies d'anàlisi, d'alternatives i objectius definits es demanarà presentar de forma estructurada, clara i concicsa els diferents models identificats com a possibles candidats a ser adquirits per a l'Agència.

En aquest punt, es presentarà tota la documentació tècnica i estadística necessària que permeti entendre els diferents models, en les seves diferents vessants, i la justificació pertinent de per què han estat les millors opcions. Addicionalment a aquestes conclusions, serà de valor que l'empresa pugui aportar la seva visió experta a través de recomanacions i arguments propis dels models i escenaris identificats com a possibles candidats.

3.11.14.4. Definició estratègica de compra en base als models seleccionats

Es podrà demanar suport i acompanyament a la definició de l'estratègia de compra i del millor canal de compra possible pels models i escenaris seleccionats en el curt, mig i llarg termini. Segons l'objecte de la compra (volumetries, productes innovadors, tipologia i criticitat del producte o servei a adquirir...) aquesta activitat haurà de contemplar possibles sessions d'innovació oberta amb les parts implicades.

3.11.14.5. Suport i acompanyament al procés de compra

Aquest servei contempla el suport i acompanyament al procés de licitació. Les activitats a executar, sense ser exhaustives ni limitatives, podran ser:

- Redacció dels documents tècnics i funcionals involucrats en la compra.
- Justificar la compra dels models seleccionats i en base a l'estratègia de compra definida aspectes com les necessitats tècniques i/o operatives i el valor econòmic.
- Identificar els criteris avaluables en la recepció de propostes per part dels candidats.

Suport en la comunicació i amb els diàlegs amb els candidats.

3.11.14.6. Generació de lliurables

Les empreses homologades que siguin adjudicatàries d'un contracte basat d'aquest tipus de serveis d'anàlisi de solucions hauran de generar lliurables de forma iterativa durant tota la durada del contracte. Aquests lliurables estaran associats a cadascuna de les fases del servei com a output i seran acordats amb l'Agència a l'inici del servei.

A mode orientatiu i no limitatiu s'hauran de generar documents com els següents:

- Anàlisis i matrius DAFOs
- Reports estadístics, gràfiques i taules comparatives
- Fitxes i informes tècnics
- Informes qualitatius amb recomanacions basades en l'experiència prèvia de l'empresa
- Plec de prescripcions tècniques
- Informes justificatius
- Reports de seguiment i control
- Etc...

Tot document podrà tenir la versió complerta amb tot tipus de detall seguit en el procés. I també es podrà sol·licitar altres versions més reduïdes i/o executives que ajudin a la presa de decisions i a compartir la informació de manera més àgil.

Rols i funcions del Lot

A títol enunciatiu i no limitatiu es defineixen els rols i les funcions que es podran sol·licitar en els posteriors contractes basats d'aquest lot de manera no acumulativa. Un mateix perfil podrà assumir més d'un rol/funció:

Nom Capacitat	Funcions
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. També serà l'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. Realitzarà funcions de direcció global. Vetllarà per la correcta coordinació dels serveis i projectes dels contractes basats, tot garantint-ne l'assoliment dels objectius. Garantirà que els equips de gestió siguin els més adequats per l'assoliment dels objectius. També participarà en els òrgans de govern del contracte d'acord amb el Model de Relació. Aquesta figura ha d'estar durant tota la durada de l'Acord Marc. Aquesta figura és obligatòria per a qualsevol empresa que s'homologui i serà comuna als eventuals contactes basats que puguin adjudicar-se a casa companyia.
Coordinador/ Cap projecte	Lideratge del basat, planificació, supervisió i coordinació dels diferents perfils implicats en la prestació de serveis del contracte. Actuar com a enllaç entre el proveïdor i els diferents agents i fabricants implicats en l'ecosistema de l'Agència. Assegurar que tot el personal de l'adjudicatari que prestarà serveis, passi per un pla de conscienciació i formació en matèria de seguretat. Assegurar que tot el personal del proveïdor que hagi de tractar dades o sistemes de tractament de dades de nivell sensible o superior signin un Acord de Confidencialitat 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. Participar en el disseny fins a la implantació dels projectes de seguretat, incloent els aspectes de compliment normatiu, liderar plans de millora, elaborar informes d'activitat, dels serveis o projectes que li siguin encomanats, dintre dels marges de qualitat, temps i cost establerts, i marcant les directrius que l'equip ha de seguir per realitzar aquestes activitats. 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 En funció del contracte basat que es tracti aquest podrà coincidir amb el responsable de l'empresa homologada.
Tècnic Especialista en anàlisi de solucions	Tècnic especialista en tecnologies en l'àmbit de la ciberseguretat, tenint en compte la innovació, disruptives i d'alt impacte, encarregat de la identificació, estudi de beneficis i viabilitat, i suport expert d'eines, productes, mesures, mètodes i metodologies, mecanismes d'automatització i tecnologies emergents.

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 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:

3.11.15. 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.

3.11.16. 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 el que estableix el Reglament General de Protecció de Dades.

Pel que fa a la seguretat en el tractament d'aquestes, l'empresa homologada implementarà les mesures de seguretat establertes per l'Agència de Ciberseguretat en el Marc de Ciberseguretat per a la Protecció de Dades. Aquesta implementació i nivell de compliment seran incorporats al model de compliment normatiu de la Generalitat de Catalunya.

3.11.17. 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.

3.11.18. 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.

3.11.19. 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.

3.11.20. 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.

3.11.21. 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.

3.11.22. 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.

3.11.23. 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 estabiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims. .

3.12 Assegurament i control de la qualitat i la millora contínua

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

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

- Anàlisi i avaluació de les dades obtingudes de la mesura del servei, tant de producció i activitat com de gestió de l'incidental i operació.
- Plans de millora del servei orientats a millorar el compliment dels objectius del servei i del negoci.
- Accions per l'assegurament i control de la qualitat (revisions, proves, etc.), amb major rigor, intensitat i profunditat segons la criticitat del projecte/servei/component.

- Accions per reduir el nombre d'incidències, problemes freqüents i el suport.
- Accions per millorar la qualitat percebuda i la satisfacció dels usuaris.
- Accions preventives per la mitigació de riscos, tenint en compte la seva probabilitat i el seu impacte.
- Accions dirigides a millorar la gestió del coneixement i incrementar la usabilitat dels serveis.
- Accions per maximitzar l'eficiència i la sostenibilitat del servei.

3.13 Seguiment del servei

Les empreses adjudicatàries dels contractes basats hauran de presentar un informe de seguiment de cada contracte basat d'acord amb els indicadors de compliment i altra informació rellevant pel seguiment del servei. Aquests informes s'avaluaran als comitès operatius i es formalitzaran i s'elevaran els seus resultats a la resta de comitès.

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

- Un informe de gestió dels serveis desenvolupats per a cada basat, amb indicació de les activitats realitzades i les previstes realitzar, les volumetries globals d'activitat i els indicadors de compliment especificats als. Acords de Nivell de Servei (ANS) de cada basat.
- Un informe de dedicació del basat a les diferents funcions requerides, per tal de poder avaluar la distribució dels esforços.
- Un informe d'accions de millora de l'activitat del propi basat, on es detallaran les accions de millora proposades amb informació rellevant per a la seva gestió (per exemple, el benefici previst obtenir, el termini d'implantació, etc.). Per cada millora implantada s'establirà, sempre que sigui possible, un indicador que s'afegirà a l'informe de gestió dels serveis. La periodicitat de l'informe de seguiment serà mensual, quant al seguiment de les activitats i la implantació de les millores. La presentació de les propostes de millora es farà amb la periodicitat indicada en cada contracte basat o el que es determini per part del responsable del contracte de l'Agència de Ciberseguretat.

Si existeix cap especificitat en aquest sentit, es recollirà al basat corresponent.

Pel control i seguiment del servei s'utilitzaran dades, mètriques i informes (en endavant informació) que serviran de suport als òrgans de gestió establerts i que són, en el seu conjunt, el mecanisme de seguiment i avaluació del servei. Aquesta informació es pot fer extensible a altres Unitats, Àrees, Direccions de l'Agència o tractar-se d'anàlisi puntual.

L'empresa adjudicatària del contracte basat és la responsable de generar i lliurar la informació que es determini en els diferents àmbits del servei, la qual ha de permetre a l'Agència governar, controlar i gestionar els serveis prestats objecte del contracte, tant des d'una òptica individual, com transversal i global.

La periodicitat, dates límit de lliurament, canals de transmissió, format exacte i contingut detallat de la informació a elaborar per l'empresa homologada 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 homologada 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 homologada hi donarà resposta ràpida fora de la planificació establerta.

3.14 Integració amb altres equips

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

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

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

- Participació de l'adjudicatari en els processos que l'afectin
- Compartició d'informació sobre fets puntuals (incidències, alertes, vulnerabilitats, 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.

3.15 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.

3.16 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.

3.11.24. 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).

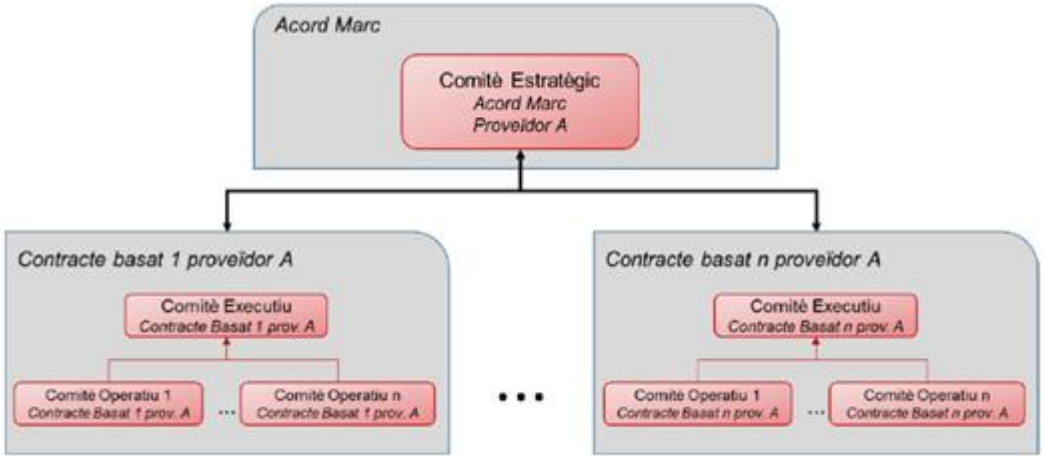
En cas que el proveïdor rebi directament alguna sol·licitud d'iniciativa o necessitat, per part d'un departament o entitat, haurà de ser redireccionada a l'òrgan gestor de l'Agència encarregat de la demanda. Per les peticions i incidències, el grau d'automatització determinarà la recepció directa d'aquestes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



3.11.25. 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.

3.11.26. 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	***Adjudicatari***
- 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.

3.11.27. 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***	***Adjudicatari***
- 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.