Plec de prescripcions tècniques particulars que regeix l'Acord Marc de serveis de suport a les funcions de Ciberseguretat pròpies del Centre d'Operacions de Seguretat de l'Agència de Ciberseguretat de Catalunya.

Lot 1: Operació de la seguretat.

Lot 2: Enginyeria de la seguretat.

Lot 3: Resposta a incidents.

Lot 4: Intel·ligència d'amenaces.

Lot 5: Anàlisi tècnic de seguretat.

Exp. AM.02.2024

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

0 INTRODUCCIÓ 1
1 DESCRIPCIÓ DELS SERVEIS OBJECTE DE L'ACORD MARC 3
2 LOT 1: OPERACIÓ DE LA SEGURETAT 8
3 LOT 2: ENGINYERIA DE SEGURETAT 11
4 LOT 3: RESPOSTA A INCIDENTS 14
5 LOT 4: INTEL·LIGÈNCIA D'AMENACES 16
6 LOT 5: ANÀLISI TÈCNIC DE SEGURETAT. 19
7 CONDICIONS D'EXECUCIÓ DEL SERVEI 20
8 MODEL DE GOVERNANÇA 31

0 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.

0.1 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.

1 Descripció dels serveis objecte de l'Acord Marc

El present Acord Marc inclou els serveis de suport al desplegament de les funcions de l'Àrea d'Operacions de la Seguretat de l'Agència.

Aquesta àrea (també coneguda internament com a SOC/CERT) s'encarrega d'executar les mesures operatives específiques per prevenir la materialització de les ciberamenaces dins dels àmbits d'actuació i de respondre, quan sigui necessari, per a reduir al màxim la seva afectació si l'incident arriba a materialitzar-se. Per fer-ho, tota l'operació de la seguretat gira al voltant del **concepte "perímetre de ciberseguretat"**, entenent-se per perímetre el conjunt d'activitats i tecnologies desplegades i governades pel SOC/CERT, que contribueixen a la millora de la ciberseguretat dels sistemes d'informació, infraestructures transversals o de les persones.

L'Àrea d'Operacions de Seguretat, s'organitza precisament en tres línies principals de Treball (també anomenades 'verticals'):

- Catalonia-SOC (de "*Security Operations Center*" en anglès)
- Catalonia-CERT (de "*Computer Emergency Response Team*" en anglès)
- Evolució, avaluació i gestió del servei SOC

Els serveis objecte de la present Acord Marc tenen com a objectiu fonamental donar suport a part del desenvolupament de les funcions i responsabilitats operatives que l'Agència de Ciberseguretat té assignades segons els marc legal i els successius encàrrecs, acords de Govern, acords de col·laboració i encàrrecs de Govern que ha rebut.

L'objecte de la present licitació té per objectius principals contribuir a la prevenció, detecció, protecció i resposta davant d'esdeveniments maliciosos, ciberatacs i incidents de seguretat que puguin afectar a l'abast d'actuació de l'Agència de Ciberseguretat, des de les línies de treball de les diferents funcions d'operació de la ciberseguretat que composen la funció de SOC/CERT.

1.1 Funcions del SOC/CERT

La següent figura mostra les 3 principals línies de treball que defineixen el SOC/CERT i reflecteix els diferents equips existents dins del SOC/CERT. Els serveis objecte del present Acord Marc es relacionaran amb la resta de funcions i amb els seus corresponents serveis de suport subjacents.

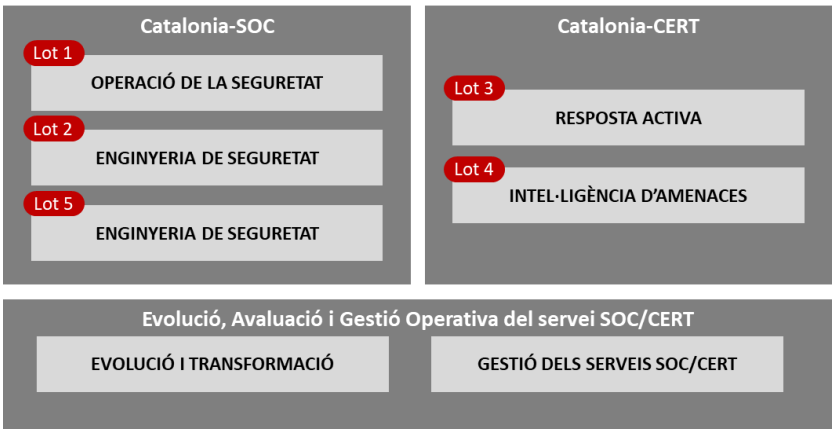


Figura 1. Funcions i subfuncions actuals del SOC/CERT

1.2 Model funcional agregat

L'estructura funcional dins del SOC/CERT, juntament amb els serveis de suport a l'operació de l'Agència de Ciberseguretat de Catalunya sobre la que es sustenta, pretenen satisfer els quatre eixos fonamentals de la seguretat de la informació enfront d'amenaces i incidents de seguretat (detecció, prevenció, protecció i resposta) i es distribueix en fins a 6 funcions diferenciades.

La distribució en funcions (amb els seus serveis de suport subjacents) té com a objectiu principal garantir la seguretat dels actius TIC de tot l'àmbit alhora que s'incrementa el nivell de maduresa actual de l'Àrea d'Operacions de Seguretat de l'Agència de Ciberseguretat de Catalunya.

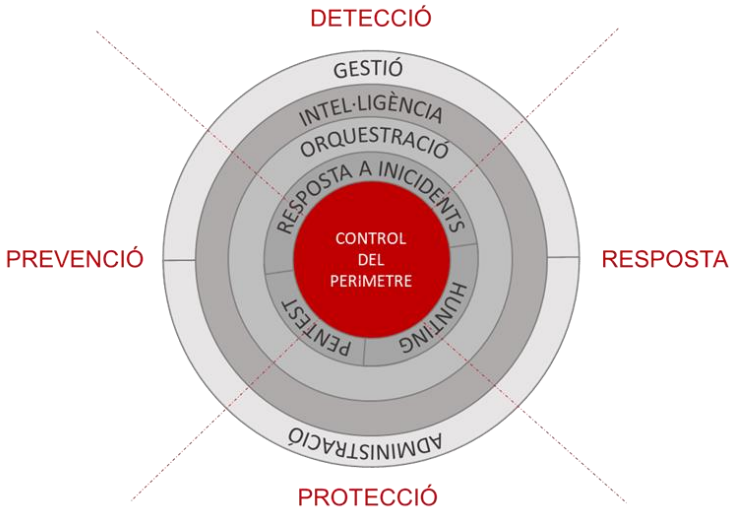


Figura 2. Estructura funcional actual del SOC/CERT

La primera funció és la de **Control i Operació del Perímetre** (COP), que dona resposta a la operació de perímetres dels eixos de detecció, prevenció i resposta. Aquesta funció correspon a tasques relatives a la gestió del cicle de vida dels esdeveniments, vulnerabilitats, amenaces i atacs de ciberseguretat fins que aquests es considerin o categoritzin com a incidents (que consisteix entre d'altres en l'anàlisi i gestió proactiva de les alertes rebudes pels dispositius de seguretat desplegats) amb l'objectiu principal de prevenir, protegir i detectar possibles atacs a la seguretat que afectin els sistemes d'informació i a la protecció davant vulnerabilitats conegudes.

Les funcions de 'Pentest' i 'Hunting' donen suport a la resta de funcions, avaluant i validant de manera proactiva els mecanismes i controls establerts respecte als quatre eixos de detecció, prevenció, protecció i resposta, per identificar punts de millora.

Tot i la efectivitat dels controls i les tasques de prevenció desplegades, encara existeix la possibilitat de que una amenaça es materialitzi en un incident de ciberseguretat. Aleshores, la funció de **Resposta Activa** (RAC) s'activa de manera reactiva quan es detecta un incident de severitat elevada, per permetre reduir en temps i forma la seva afectació dins de l'àmbit i per garantir que el mateix tipus d'incident no torna a succeir en les mateixes circumstàncies.

Al voltant de les funcions més operatives del SOC/CERT es desplega la funció d'Orquestració Operativa que permet garantir que tots els esforços dels diferents equips es centren en tot moment en els mateixos focus. Respecte a l'operació recurrent, l'orquestració també permet assegurar que

per cada element a tractar (bé sigui una vulnerabilitat, un atac, un incident o una nova amenaça), es treballa sempre des d'un punt de vista construït sobre l'amenaça com a element central (*Threat-Centric*), el que permet assegurar tots els requeriments necessaris per una prevenció i una resposta efectiva i amb garanties.

De manera recurrent es porten a terme reunions operatives dins del SOC/CERT on totes les funcions i els seus serveis corresponents acorden les tasques a executar i els principals focus operatius, evolutius i incidentals sobre els que s'han de concentrar els recursos disponibles.

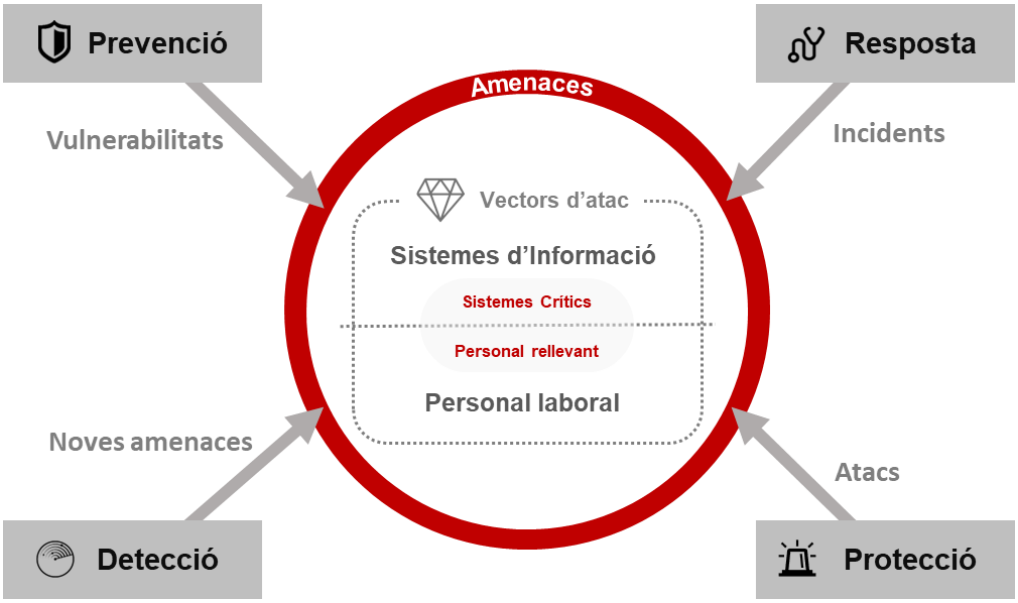


Figura 3. Plantejament "Threat-Centric"

Justament per sobre de l'Orquestració Operativa, es desplega la funció d'**Intel·ligència d'Amenaces**, que complementa l'activitat de les funcions anteriors, amb una visió orientada a l'anàlisi del context de la ciberseguretat de l'organització i l'àmbit d'actuació de l'Agència de Ciberseguretat.

A partir de la informació resultant de l'operativa de les diferents funcions prèviament citades i els seus serveis de suport, d'altres entitats de l'àmbit de la ciberseguretat i de fonts externes de coneixement, es realitza una correlació i anàlisi en profunditat per tal de determinar patrons d'actuació i potencials noves ciberamenaces. Aquestes tasques s'associen a totes les fases de la 'Cyber Kill Chain' del MITRE i també es realitza una tasca analítica de la operativa resultant de la resta de funcions.

Aquesta correlació i anàlisi de la informació es realitza amb l'objectiu de definir una estratègia que sigui efectiva al llarg del temps mitjançant la retroalimentació dels resultats. Amb això es pretén evitar que aquestes ciberamenaces identificades es materialitzin en incidents de seguretat que puguin posar en perill qualsevol actiu dins de l'àmbit d'actuació de l'Agència de Ciberseguretat

Addicionalment, de manera transversal, la funció de "**Enginyeria de seguretat**" (ENS) que principalment aporta i garanteix la disponibilitat de les solucions tecnològiques que donen resposta a les necessitats de tota l'Agència de Ciberseguretat de Catalunya.

Per últim, de manera transversal i fora de l'abast d'aquest Acord Marc, la funció de "Governança i Evolució de l'Operació" permet evolucionar el SOC/CERT, garantir la gestió eficaç dels recursos i

capacitats de les diferents funcions del SOC/CERT, i posar en valor tota l'activitat operativa portada a terme pels seus equips.

1.3 Elements bàsics d'execució

A banda de les funcions i tasques pròpies de cada servei, que s'especificarà en cadascun dels contractes basats en l'Acord Marc, 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 ambdós 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.
- Generar els indicadors, informes d'activitat i mesures de l'impacte d'aquesta activitat.
- Definició, creació, distribució i manteniment dels informes del servei i de risc derivats de l'activitat.
- Realitzar anàlisis i proves de les eines que es considerin oportunes per a la millora o industrialització del servei.
- Proposar millores, mantenir i, si s'escau construir les metodologies pròpies de treball del elements de servei objecte de licitació.
- 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 Lot 1: Operació de la seguretat

2.1 Objecte

L'objectiu principal d'aquest servei és operar i governar les diferents fronteres de ciberseguretat definides i desplegades als diferents àmbits competència de l'Agència. D'aquesta manera, a les empreses homologades se'ls exigirà el suport a l'Agència en totes les tasques pròpies i contínues de prevenció, detecció, protecció i resposta al perímetre pel qual ha de garantir la seguretat.

En aquest sentit, és important recordar que, per a l'Agència, les operacions de seguretat giren al voltant del concepte de "perímetres de ciberseguretat", entenent com a tal el conjunt d'activitats i tecnologies desplegades i gestionades per l'àrea d'Operacions que ajuden a millorar la ciberseguretat dels sistemes d'informació, les infraestructures transversals o les persones.

En aquest context, ia mode d'exemple no limitatiu, entre les funcions que es podran exigir a les empreses homologades hi ha:

1. **Gestió de perímetres de seguretat:** En aquesta funció s'ha de donar suport, entre d'altres, a tota la monitorització i la gestió corresponent d'alertes de seguretat que permetin identificar potencials amenaces, atacs o incidents de seguretat sobre actius en perímetre. Això inclou, entre d'altres: Revisió i seguiment constant dels esdeveniments de seguretat notificats per les solucions de seguretat, manteniment dels procediments operatius que determinen la resposta a les diferents tipologies d'alertes, la definició i la sol·licitud de noves regles de correlació/protecció sobre solucions de seguretat perimetral, així com el control sobre l'activitat de seguretat produïda en els actius de l'abast.
2. **Prevenció d'amenaces:** Aquesta funció inclou, a títol enunciatiu, l'anàlisi de tota la informació de context disponible de ciberamenaces aplicables als àmbits dins de l'abast i la corresponent execució de tasques per prevenir la materialització de l'amenaça als actius. Entre altres, s'inclouen activitats com: Anàlisi de tendències, patrons i anomalies per determinar possibles incidents, revisió d'informes i resultats generats per altres equips o eines que permetin determinar el grau d'exposició a les amenaces identificades, així com el desplegament de contramesures a les eines perimetrals que permetin evitar o minimitzar l'impacte de les amenaces esmentades.
3. **Protecció davant de ciberatacs** : En aquesta funció s'haurà de donar resposta a aquells esdeveniments significatius que suposin o puguin suposar un potencial incident de seguretat. Això inclou: aplicació o sol·licitud d'aplicació de contramesures per evitar o reduir l'impacte sobre l'abast del basat, l'escalat de casos complexos a altres grups resolutoris, així com la participació en tot el procés de gestió dels casos, inclosos el seguiment i el suport en comitès de crisi quan sigui necessari.
4. **Identificació, anàlisi i gestió de vulnerabilitats** : Aquesta funció serà responsable de la identificació de vulnerabilitats de seguretat en els àmbits de treball dins de l'abast, així com el seguiment del cicle de vida complet dels aspectes identificats per assegurar-ne la correcció. Això inclou la realització d'anàlisis de seguretat puntuals i periòdiques sobre els actius en l'avenç, registre, validació i reporti dels resultats obtinguts, definició de possibles mesures a aplicar per a la mitigació de vulnerabilitats, així com el seguiment i comprovació de la correcta aplicació aquestes accions correctores.

Addicionalment, en algun cas, s'haurà d'oferir el suport i el govern d'altres equips que requereixin executar accions similars en altres àmbits o entorns més acotats on la capacitat d'execució directa de mesures operatives sigui limitada.

Així mateix, les empreses homologades esmentades també seran responsables de donar visibilitat de l'activitat generada pel mateix servei en temps real als diferents àmbits en què l'Agència presta servei.

2.2 Rols i funcions

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

- Analistes de seguretat: responsables dels casos d'ús i alertes de seguretat, protocols d'actuació, millora de regles de detecció, anàlisi de patrons, millora de *playbooks* , industrialització.
- Experts en vulnerabilitats: responsables de la gestió en tot el cicle de vida de les vulnerabilitats detectades pel servei tant automàticament com manualment.
- Experts en amenaces: responsables de la informació provinent de les amenaces per poder interpretar i relacionar amb vulnerabilitats i atacs que ajudin a determinar el grau d'exposició dels actius, així com identificar anomalies, tendències rellevants, etc.
- Experts en gestió d'atacs i incidents autogestionats: responsables experts en atacs de ciberseguretat, definició d'escalats i tractament dels incidents detectats, suport i anàlisi, comitès de crisi. En funció de la complexitat de l'atac o incident, en el contracte basat es poden diferenciar diferents nivells de capacitació (N1, N2, N3).
- Responsable/Cap de servei: encarregat de liderar i coordinar el servei a tots els àmbits, generació d'informes executius, així com liderar la integració operativa dels àmbits, entitats i altres SOC/CERT. El perfil s'especifica posteriorment al capítol corresponent a condicions d'execució del servei.

A continuació, es presenten els coneixements desitjables dels perfils professionals que compondran els equips:

Rol	Coneixements
Analista de seguretat	• Coneixements tècnics en elements de seguretat, sistemes operatius, xarxes, protocols i programari. • Coneixements per al tractament i resposta davant d'esdeveniments i incidents de seguretat. • Coneixements a nivell analític per abastar tot l'escenari d'un incident.
Experts en vulnerabilitats	• Coneixements tècnics relacionats amb els processos d'identificació, anàlisi i gestió de vulnerabilitats de seguretat. • Coneixements tècnics d'elements de seguretat, sistemes d'informació heterogenis, xarxes, programari, protocols de comunicacions, etc. • Coneixements sobre vulnerabilitats i debilitats tècniques més freqüents, així com mètodes per a la seva explotació, solució, mitigació o contenció, incloent problemes de seguretat física, errors de disseny en protocols, programari maliciós, errors d'implementació, debilitats de configuració, errors o indiferència dels usuaris, entre d'altres.
Experts en amenaces	• Coneixements tècnics en investigació i anàlisi d'amenaces i atacs. • Coneixements tècnics dels elements de seguretat.

Rol	Coneixements
Experts en gestió d'atacs i incidents autogestionats	• Coneixements relacionats amb laplicació de metodologies i operació deines de monitorització i protecció perimetral. • Coneixements per al tractament i resposta davant d'esdeveniments i incidents de seguretat. • Coneixements en tècniques de seguretat de xarxes, incloent seguretat perimetral, seguretat de routers, monitorització de trànsit, entre d'altres. • Coneixements d'elements de seguretat, sistemes operatius, bases de dades, programari de control, programari de treball.

2.3 Lliurables del servei

La prestació de qualsevol servei inclòs en aquest Lot podrà requerir de manera no limitativa la preparació per part de les empreses homologades d'una sèrie de lliurables, com ara informes sobre l'estat de les infraestructures, resums de l'activitat dels serveis, detall dels incidents /problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans dacció o planificacions, riscos operatius, notificacions, mètriques i indicadors, entre altres.

Aquests lliurables es concretaran en cada contracte basat, així com la seva periodicitat i contingut mínim.

3 Lot 2: Enginyeria de Seguretat

3.1 Objecte i abast

L'objectiu principal d'aquest servei és administrar i mantenir les solucions tecnològiques de seguretat emprades per l'Agència en els diferents àmbits per poder donar una resposta adequada a les funcions que han de desenvolupar els diferents serveis i necessitats de l'Agència, tant en la correcta posada a punt com a les necessitats funcionals.

Addicionalment, les empreses homologades s'encarregaran de vetllar pel desplegament de les funcions requerides que donin resposta al model de perímetre de seguretat definit per l'Agència als diferents àmbits, a partir de la integració tecnològica de solucions que puguin disposar els àmbits amb les de l'Agència.

Aquest servei tindrà associat un conjunt de funcions transversals, l'objecte de les quals serà vetllar per l'excel·lència operativa en termes d'eficiència i eficàcia tant tècnica com econòmica, la millora contínua dels serveis i la satisfacció dels clients de l'Agència.

De forma no limitativa, les funcions que es requeriran a les empreses homologades inclouen:

1. **Governança del servei.** Aquesta funció serà l'encarregada de governar i dirigir tècnicament (elaborar directrius) les solucions de seguretat de perímetre tant les pròpies, per desenvolupar tots els serveis de la Agència, com dels seus diferents àmbits de manera que proporcionin un suport adequat a les vostres necessitats i requisits de seguretat. Això inclou activitats com: Manteniment d'inventari de solucions/cas d'ús/fonts, gestió de polítiques, control de les llicències, versions de programari, manteniment de persones de contacte de fabricant, gestió de la demanda interna, mapeig de les solucions a les àrees de prevenció, protecció, detecció i resposta d'amenaces, gestió i interlocució amb fabricants i integradors de solucions, constituir la cara visible del servei participant a les reunions que siguin requerides en relació amb solucions de seguretat de l'Agència o els seus àmbits (orquestració, comitès de crisi, etc.), així com fer suport i guia dels projectes d'implantació de les solucions de ciberseguretat.
2. **Enginyeria solucions seguretat:** La funció principal és administrar, configurar i gestionar les solucions de ciberseguretat en l'àmbit del contracte basat amb l'objectiu que donin resposta satisfactòria a les necessitats funcionals i de seguretat que es requereixin. Això inclou: Manteniment i posada a punt, actualització i pegat, creació de quadres de comandament, automatitzacions, integracions i industrialitzacions sobre les eines o solucions utilitzades. Addicionalment, inclourà el suport a altres serveis que utilitzin les solucions de seguretat, així com el suport i resolució d'incidències i problemes, incloent-hi la gestió amb els fabricants de les solucions de seguretat per resoldre aquests problemes en cas que no es puguin resoldre directament per la pròpia funció.
3. **Desplegament del perímetre:** L'Agència disposa de diferents modelitzacions per assegurar els diferents vessants de prevenció, protecció, detecció i resposta d'amenaces, referits com a perímetres. Aquesta funció serà l'encarregada de controlar que el desplegament de perímetres de l'Agència o els seus àmbits es faci conforme a aquests models, verificant que cada funció de seguretat és coneixedora dels requisits del perímetre i assegurant que aquesta funció li reporta convenientment l'estat i els avenços en el desplegament. Això inclou, entre d'altres, les activitats següents: Comunicar els requisits d'implantació del perímetre per a la solució de seguretat i controlar-ne el compliment, gestionar les integracions amb elements de seguretat de l'Agència (SIEM, escaneig d'infraestructura i aplicacions, etc.), parametritzar les solucions de seguretat que correspongui per la inclusió d'actius a desplegar al perímetre de seguretat, realitzar control i seguiment de les peticions en curs relacionades amb el desplegament de perímetre, així com assegurar una adequada gestió del coneixement en relació amb el desplegament del perímetre.

3.2 Rols i funcions

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

- Enginyers de seguretat: responsables tècnics de les solucions de ciberseguretat.
- DevOps: responsables del desenvolupament de millores de capacitats de les eines, automatitzacions de processos i integracions entre les diferents solucions, generació de quadres de comandament operatius (*dashboards*), etc.
- Responsable/Cap de servei: encarregat de liderar i coordinar el servei en tots els àmbits i generar informes executius. El perfil s'especifica posteriorment al capítol corresponent a condicions d'execució del servei.

A continuació, es presenten els coneixements desitjables dels perfils professionals que compondran els equips:

Rol	coneixements desitjables
Enginyers de seguretat	• Coneixements tècnics d'amenaces i vectors d'atac. • Coneixement de sistemes de seguretat tant tradicionals com emergents. • Coneixements tècnics de xarxes, programari, protocols de comunicació, etc. • Coneixements en la configuració segura dels sistemes. • Coneixements de vulnerabilitats i defectes a què poden estar subjectes infraestructures, plataformes i aplicacions.
DevOps	• Coneixements en implantació, administració, manteniment i integració de solucions de seguretat. • Coneixements en diferents llenguatges de programació que permeti fer automatitzacions i integracions. • Coneixements en resolució de problemes i incidències. • Coneixement de ferramentes de gestió i quadres de comandament. • Coneixement de ferramentes d'automatització.

Les empreses homologades han de dotar els equips humans amb les capacitats tècniques, les eines, les habilitats i les estructures organitzatives per donar suport a l'Agència en la prestació dels serveis tècnics d'enginyeria de seguretat.

3.3 Lliurables del servei

La prestació de qualsevol servei inclòs en aquest lot requerirà la preparació per part de les empreses homologades d'una sèrie de lliurables, com a informes descrivint les funcions del servei, resum de les activitats mensuals del servei, detalls dels incidents/problemes més importants durant el període, seguiment de resolució de problemes, enquestes de satisfacció per als lliurables, estat de projectes, planificació i plans dacció, entre altres. Aquests lliurables es concretaran en cada contracte basat, així com la seva periodicitat i contingut mínim.

4 Lot 3: Resposta a incidents

4.1 Objecte i abast

L'objectiu principal d'aquest servei és executar el conjunt d'activitats i tecnologies desplegades pel SOC/CERT per fer front als incidents de seguretat, tant de manera proactiva com reactiva per garantir que no tornin a succeir. Addicionalment ha de garantir la gestió correcta de les evidències i la validesa jurídica, així com proveir el coneixement i els plans d'actuació necessaris per reduir de manera efectiva i eficient l'impacte de les ciberamenaces dins els àmbits d'actuació de l'Agència.

En aquest context, ia mode d'exemple no limitatiu, entre les funcions que es podran exigir a les empreses homologades hi ha:

1. **Resposta a incidents** : Funció responsable de respondre de forma diligent a incidents de seguretat en temps i forma minimitzant l'impacte, assegurant-ne l'eradicació i garantint que no es puguin tornar a repetir de la mateixa manera. Per això s'encarregarà de tota la coordinació de la crisi, així com de proveir el relat necessari respecte a la investigació per a la presa de decisions en el context d'un incident . Les tasques de la funció inclouen, entre d'altres: Recopilació i ordre cronològic de tota la informació i evidències generades, coordinació dels diferents equips participants a la resposta d'incidents, gestió i lideratge dels diferents comitès de crisi.
2. **Anàlisi forense :** En aquesta funció s'executaran les diferents anàlisis tècniques derivades d'incidents o campanyes de cerca proactiva d'amenaces per reduir l'impacte en cas d'incident, determinar les causes d'un incident per evitar que es pugui tornar a repetir i proveir el context necessari que ajudi a la presa de decisions als diferents comitès. Per això haurà de recopilar, analitzar i emmagatzemar les evidències seguint un procés que garanteixi la integritat d'aquestes i de la seva cadena de custòdia garantint-ne la validesa davant un possible procés judicial. Això inclou tasques com: anàlisi de codi maliciós, anàlisi forense de diferents tipus de dispositius i tecnologies, proposta de plans d'eradicació i recuperació en el context d'un incident, extracció d'indicadors sobre la base de l'anàlisi forense, inventariat i control de les evidències recol·lectades, així com el registre i documentació dels resultats de les investigacions realitzades.

3. **Cerca proactiva d'incidents** : En aquesta funció es realitzaran tasques de cerca proactiva d'amenaces (*Threat Hunting*) per detectar possibles incidents no detectats pels sistemes de detecció desplegats. El servei requereix una metodologia, estratègia i planificació amb aquesta finalitat, que a més permeti mesurar el grau de preparació de les diferents entitats davant d'un potencial incident. Les tasques inclouen, entre d'altres: detecció d'anomalies, correlació avançada d'esdeveniments, definició de recomanacions i propostes de millora segons les campanyes realitzades. Addicionalment, aquesta funció serà responsable de mantenir i evolucionar les eines i els procediments necessaris per dur a terme aquestes tasques.

4.2 Rols i funcions

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

- Experts d'incidents (*incident handler* , analista DFIR): responsables de la gestió d'incidents complexos en tota mena d'infraestructures, així com del lideratge tècnic de les diferents anàlisis forenses derivades dels incidents o de les campanyes de cerca proactiva d'amenaces.
- Tècnics de resposta a incidents (analista DFIR): encarregats de la realització de les diferents

anàlisis. La seva funció és la realització d'anàlisis forenses i la implementació tècnica de tasques dins de la resposta a incidents, a més d'assegurar una gestió correcta d'evidències per garantir-ne la integritat. A més a més de la component reactiva, són els encarregats de l'execució de les diferents tasques proactives de cerca d'indicis que puguin evidenciar la materialització d'incidents.

- Responsable/Cap de servei: encarregat de liderar i coordinar el servei, generació d'informes executius, així com liderar la integració operativa dels àmbits, entitats i altres SOC/CERT. El perfil s'especifica posteriorment al capítol corresponent a condicions d'execució del servei.

A continuació, es presenten els coneixements desitjables dels perfils professionals que compondran els equips:

Rol	coneixements desitjables
Experts de gestió d'incidents	• Coneixements en gestió i resposta d'incidents. • Coneixements en gestió d'equips de resposta a incidents i comitès de crisi. • Coneixements que permetin la planificació, el desplegament, el seguiment i la millora de la resposta a incidents de ciberseguretat. • Coneixement per al desenvolupament de procediments generals per respondre a incidents de ciberseguretat. • Coneixements tècnics relacionats amb metodologies i eines d'anàlisi forense. • Coneixements en gestió de cadena de custòdia.
Tècnics de resposta a incidents	• Coneixements en resposta a incidents de seguretat. • Coneixements tècnics relacionats amb metodologies i eines d'extracció i anàlisi forense. • Coneixements en gestió de cadena de custòdia. • Coneixements tècnics per a la investigació en solucions de seguretat. • Coneixements tècnics sobre vulnerabilitats i debilitats tècniques més freqüents. • Coneixements de sistemes operatius, xarxes, bases de dades, programari i monitorització.

4.3 Lliurables del servei

La prestació de qualsevol servei inclòs en aquest lot requerirà la preparació per part de les empreses homologades d'una sèrie de lliurables, com a investigació d'incidents i el seu suport com a anàlisi forense o de *malware* , la seva presentació executiva, cerca proactiva d'incidents, resums mensuals de l'activitat dels serveis, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscs operatius, mètriques i indicadors, entre d'altres. Aquests lliurables es concretaran en cada contracte basat, així com la seva periodicitat i contingut mínim.

5 Lot 4: Intel·ligència d'amenaces

5.1 Objecte i abast

Aquest servei s'encarregarà de proporcionar el coneixement i els plans d'actuació necessaris per permetre reduir de manera efectiva i eficient l'afectació d'amenaces als àmbits d'actuació de l'Agència.

Les tasques a realitzar han de permetre generar criteri sobre ciberamenaces que es puguin convertir en un potencial incident de seguretat, així com habilitar, de manera natural, la presa de decisions. Els resultats es produiran a partir de la cerca i el processament de la informació existent en totes aquelles fonts disponibles i serviran de base per fer un seguiment i disposar d'un històric de les ciberamenaces identificades.

A tall d'exemple no limitatiu, entre les funcions que es podran exigir a les empreses homologades hi ha:

1. **Identificació i seguiment de ciberamenaces** : Aquesta funció és l'encarregada d'identificar, analitzar i fer seguiment de les ciberamenaces més rellevants aplicables als entorns i àmbits a l'abast del basat, a partir de diferents fonts d'informació. Entre altres qüestions, inclou: la definició de directives per a la detecció d'esdeveniments rellevants per a la prevenció i resposta a ciberamenaces, l'adquisició, el processament i l'anàlisi de la informació adquirida des de diferents fonts d'informació (per exemple eines de 'Threat Intelligence', coneixement propi, fonts especialitzades o resultats generats per l'activitat de la resta d'equips operatius del SOC/CERT), identificació de les principals amenaces aplicables a l'àmbit d'abast a partir dels esdeveniments identificats, fer un pronòstic de la seva evolució, així com la determinació i seguiment del grau dexposició a les mateixes. Addicionalment, la difusió i l'intercanvi d'informació de ciberintel·ligència (tant internament com externament), prestació de suport a altres serveis en cas d'incident de seguretat o crisi rellevant per a la contextualització i definició de mesures de prevenció i contenció d'amenaces.
2. **Govern d' estratègies de resposta** : Aquesta funció és la responsable de desenvolupar, distribuir i valorar el compliment de les estratègies de resposta a tot el SOC/CERT dirigides a reduir de manera efectiva i eficient l'afectació d'amenaces. Això inclou: Definició de directrius de resposta per a les principals situacions de crisi, la seva difusió a les parts implicades, així com la seva validació activa per verificar-ne l'adequació i l'aplicació adequada en els processos operatius del SOC/CERT.
3. **Assegurament i evolució de l'ecosistema CTI** : En aquesta funció s'inclou l'administració, configuració, operació i evolució d'aquelles solucions tecnològiques d'intel·ligència d'amenaces emprades per l'Agència per demanar, tractar i compartir tota la informació relacionada amb les ciberamenaces, emprada per desenvolupar-les totes les funcions anteriors. Addicionalment, es podria requerir a l'empresa homologada que disposi de tecnologies específiques que actuïn com a fonts d'informació de valor per a la funció d'"Intel·ligència d'Amenaces".

Així mateix, el servei de forma global haurà de vetllar perquè l'operació de tots els equips del SOC/CERT utilitzi com a element vehicular l'amenaça (Threat Centric) i es desenvolupi segons les estratègies de resposta definides.

5.2 Rols i funcions

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

- Analistes d'intel·ligència: responsables d'analitzar i gestionar les alertes i deteccions provinents de les diferents fonts d'intel·ligència que pugui disposar el SOC/CERT (per exemple, *feeds* especialitzats, eines de *Threat Intelligence* , notificacions externes, investigacions pròpies o cerca manual avançada).
- Experts en amenaces: responsables d'identificar i donar visibilitat de les tendències d'amenaces que afecten els àmbits d'actuació del contracte basat, així com fer seguiment actiu de les amenaces i els actors més rellevants, determinant el grau d'exposició del conjunt d'actius o entitats a aquestes amenaces. Addicionalment, prestaran suport per a l'entesa de qualsevol amenaça a la resta de serveis operatius que requereixin més context per desenvolupar les seves funcions.
- Responsables infraestructura CTI (DevOps): responsables que les plataformes de l'ecosistema CTI del SOC/CERT ofereixin unes capacitats d'acord amb els requisits funcionals i tecnològics de la prestació del servei.
- Responsable/Cap de servei: encarregat de liderar i coordinar el servei a tots els àmbits, generació d'informes executius, així com liderar la integració operativa dels àmbits, entitats i altres SOC/CERT. El perfil s'especifica posteriorment al capítol corresponent a condicions d'execució del servei.

A continuació, es presenten els coneixements desitjables dels perfils professionals que compondran els equips:

Rol	coneixements desitjables
Analistes d'intel·ligència	• Coneixements en processament i anàlisi de múltiples fonts dinformació per a la identificació de ciberamenaces rellevants. • Coneixements de les principals amenaces a l'àmbit de la ciberintel·ligència. • Coneixements d'elements i de solucions tecnològiques de seguretat. • Coneixements analítics per abastar tot l'escenari d'una amenaça.
Experts en amenaces	• Coneixements en la investigació i l'anàlisi d'amenaces i vectors d'atac. • Coneixements en detecció de noves fonts dinformació (xarxes socials, fòrums, estudis daltres institucions, etc.) per a lanàlisi de ciberamenaces, vulnerabilitats, incidents de seguretat, etc. • Coneixements en eines de recerca i anàlisi dinformació. • Coneixements en metodologies de resposta davant d'incidents i ciberamenaces. • Coneixements a TTP (Tècniques, Tàctiques i Procediments) dels principals actors d'amenaça, així com en mesures de detecció i mitigació.
Responsable d'infraestructura CTI (DevOps)	• Coneixements en desenvolupament, implantació i administració de solucions d'intel·ligència d'amenaces 'open source' i de diferents fabricants de referència al mercat. • Coneixements de sistemes operatius, xarxes, bases de dades, programari de control, programari de treball, programari de seguretat perimetral i monitorització.

5.3 Lliurables del servei

La prestació de qualsevol servei inclòs en aquest lot requerirà la preparació per part de les empreses homologades d'una sèrie de lliurables, com informes relatius a prevenció i resposta davant d'amenaces, estratègies de resposta, exercicis d'avaluació de l'exposició a l'amenaça, pronòstics d'amenaces, resums mensuals de l'activitat dels serveis, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres . Aquests lliurables es concretaran en cada contracte basat, així com la seva periodicitat i contingut mínim.

6 Lot 5: Anàlisi tècnic de seguretat.

6.1 Objecte i abast

L'objectiu principal d'aquest servei és la detecció de vulnerabilitats i el diagnòstic de la seguretat en els diferents àmbits d'actuació de l'Agència mitjançant la replicació de tècniques utilitzades per un atacant.

En aquest sentit, es pretén conèixer l'impacte que tindrien les diferents amenaces sobre l'àmbit d'actuació fixat en el contracte basat. D'aquesta manera, proveeix el relat i les dades necessàries orientades també a la millora de les diferents capacitats de seguretat per evitar que una amenaça real que utilitzi les mateixes tècniques pugui impactar.

En aquest context, es podrà exigir a les empreses homologades la funció següent:

> **Diagnòstic de Seguretat**: Aquesta funció té la responsabilitat d'identificar la possible exposició a ciberamenaces dels actius i sistemes mitjançant la cerca de vulnerabilitats no identificades per la funció d'Identificació, anàlisi i gestió de vulnerabilitats". Això inclou: Proves d'intrusió avançades com poden ser 'pentests', anàlisi de codi font, anàlisi d'infraestructures, tests de 'phishing', entre d'altres, així com la corresponent generació de registres de resultats, proves de concepte, proposta de plans de acció per mitigar els aspectes identificats i seguiment de les accions correctives.

Així mateix, les empreses homologades esmentades també seran responsables de donar visibilitat de l'activitat generada pel mateix servei en temps real als diferents àmbits en què l'Agència presta servei.

6.2 Rols i funcions

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

- Experts de seguretat (pentester): responsables del desenvolupament d'anàlisis tècniques de penetració de diferents tipus, ja sigui per analitzar la superfície d'exposició com per detectar punts de millora.
- Responsable/Cap de servei: encarregat de liderar i coordinar el servei a tots els àmbits, generació d'informes executius, així com liderar la integració operativa dels àmbits, entitats i altres SOC/CERT. El perfil s'especifica posteriorment al capítol corresponent a condicions d'execució del servei.A continuació, es presenten els coneixements desitjables dels perfils professionals que compondran els equips:

Rol	coneixements desitjables
Expert de seguretat (pentester)	• Coneixements en metodologies i eines per a la realització d'anàlisis de vulnerabilitats i pentesting. • Coneixements que permetin aplicar tècniques d"evasió sobre els sistemes de seguretat implantats. • Coneixements sobre vulnerabilitats i debilitats tècniques més freqüents, així com mètodes per a la seva explotació, solució o accions mitigadores o de contenció, incloent problemes de seguretat física, errors de disseny en protocols, programari maliciós, errors d'implementació, debilitats de configuració, errors o indiferència dels usuaris, entre d'altres.

6.3 Lliurables del servei

La prestació de qualsevol servei inclòs en aquest lot requerirà la preparació per part de les empreses homologades d'una sèrie de lliurables, com informes relatius a prevenció i resposta davant d'amenaces, estratègies de resposta, exercicis d'avaluació de l'exposició a l'amenaça, pronòstics d'amenaces, resums mensuals de l'activitat dels serveis, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres . Aquests lliurables es concretaran en cada contracte basat, així com la seva periodicitat i contingut mínim.

7 Condicions d'execució del servei

7.1 Horaris

Atenent a la naturalesa d'alguns dels serveis inclosos en aquest Acord Marc, l'Agència pot requerir que la seva prestació es dugui a terme en un horari 24x7 365 dies a l'any. En aquests casos s'indicarà aquesta necessitat en la contractació basada.

Adicionalment, s'informa que els serveis inclosos en aquest Acord Marc poden implicar la necessitat de dur a terme (i) guàrdies i (ii) feines fora d'horari. En aquest sentit:

- Es considera guàrdia la disponibilitat per atenció telefònica i actuació presencial en horari no laboral en el cas d'actuacions especials o que la importància de la incidència ho requereix.
- A petició expressa de l'Agència, es podria demanar la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

7.2 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.

7.3 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.

7.4 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.

7.5 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

7.6 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.

7.7 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.

7.8 Formació

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

7.9 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.

7.10 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.

7.11 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.

7.12 Seguretat

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

7.12.1 Deure de confidencialitat

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

L'empresa homologada ha de comunicar aquesta obligació de confidencialitat al seu personal ja sigui intern com extern, que estigui involucrat en l'execució del contracte i possibles subcontractistes i ha de controlar el seu compliment.

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

7.12.2 Dades de caràcter personal

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

7.12.3 Compliment del marc legal de ciberseguretat i el 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.

7.12.4 Capacitat tècnica

Per a poder executar el contracte i oferir garanties de la seva capacitat tècnica, l'empresa adjudicatària del contracte basat haurà de presentar compromís exprés d'adscripció al contracte

dels mitjans personals que s'especifiquin als plecs, complint amb els requeriments definits de formació, i acreditar la disposició efectiva dels mateixos.

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

7.12.5 Adquisició de productes/eines i productes o serveis de seguretat

Tant en el cas que es desenvolupin productes/eines, es facin integracions amb altres eines o s'adquireixin eines de mercat o qualsevol component de sistemes d'informació (hardware, software, 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.

7.12.6 Interconnexions

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

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

7.12.7 Verificació del compliment i auditoria

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

7.12.8 Incidents de seguretat

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

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

7.12.9 Accés a la informació

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

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

7.13 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.

7.14 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 com a mínim de forma trimestral.

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.

7.15 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.

7.16 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.

7.17 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.

8 Model de governança

8.1 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.

8.2 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.

8.3 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.

8.3.1 Alineació amb objectius estratègics

La Direcció de l'Agència estableix una sèrie d'objectius a nivell estratègic basats en la visió, missió i valors de l'entitat, i els responsables que coordinen els serveis estableixen quins resultats clau contribuiran a aquests objectius i a quin equip involucrar per assolir-los. Aquests vindran fixats per una sèrie d'indicadors que permetin mesurar el grau de compliment al llarg del temps dels objectius. Aquest objectius seran mesurables, específics, clars, coherents, realistes i oportuns. D'aquesta

manera contribueixen a materialitzar l'estratègia, ajudar a establir les fites i avaluar el compliment, i a crear una alineació de tota l'organització.

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

8.4 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).

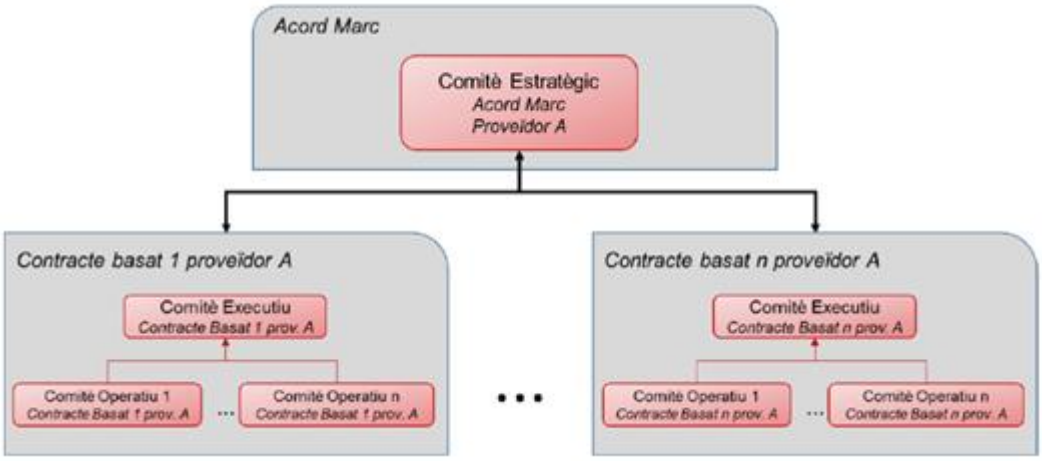
En cas que el proveïdor rebi directament alguna sol·licitud d'iniciativa o necessitat, per part d'un departament o entitat, haurà de ser redireccionada a l'òrgan gestor de l'Agència encarregat de la demanda. Per les peticions i incidències, el grau d'automatització determinarà la recepció directa d'aquestes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

8.5 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:



8.5.1 Comitè Estratègic Acord Marc

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

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

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

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

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

Responsable d'empresa homologada

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

Entre les seves responsabilitats podem destacar:

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

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

8.5.2 Comitè Executiu Contractes Basats

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

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

- Informes i quadres de comandament de seguiment - Actes comitè operatiu contracte basat - Decisions a prendre	- Acta (signada entre les parts) - Decisions preses - Propostes pel comitè estratègic de l'AM - Propostes per l'Òrgan de Contractació mitjançant el comitè estratègic de l'AM
Periodicitat	
Trimestral o a petició de l'Agència	

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

Cap de serveis del contracte

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

8.5.3 Comitè Operatiu Contractes Basats

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

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

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

8.6 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.