Plec de prescripcions tècniques particulars que regeix la contractació basada relativa al suport pel servei d'Avaluació de l'Exposició de l'Agència en l'àmbit dels Sistemes d'Informació Crítics de la Generalitat de Catalunya, estructurada en 2 lots

Lot 1: Avaluació de SICs dels departaments de PRE, ISP i ECF

Lot 2: Avaluació de SICs de tots els departaments tret de les especificades en el Lot 1

Exp. CB25AMOPL5001

Índex

1 Introducció

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència), establerta sota el marc de la Llei 15/2017, del 25 de juliol, és l'entitat que lidera i coordina els esforços de la Generalitat de Catalunya en la protecció de la informació i les infraestructures del país davant les ciberamenaces. En un món digitalitzat i interconnectat, la seguretat de la informació s'ha convertit en una prioritat estratègica, i l'Agència subratlla el compromís de Catalunya amb la promoció d'un entorn digital segur i de confiança.

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 *segons recull la memòria de l'Agència de Ciberseguretat de Catalunya de 2023, l'entitat ha tingut un paper rellevant en les tasques de resposta i coordinació per a la gestió d'incidents de seguretat durant el 2023, tant pel que fa a la Generalitat com en diferents entitats del territori català.* En aquest sentit, l'Agència gestiona més de 2.200

sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants. Aquest perímetre protegit provoca un alt nivell d'activitat de gestió. Més concretament, el nombre de ciberatacs rebuts durant l'any 2023 va ser de més de 5.000 milions, en contraposició als 4.400 milions d'atacs del 2022. Pel que fa als incidents de seguretat, l'Agència en va gestionar prop de 2.670 durant el 2023, en comparació amb els 2.175 de l'exercici anterior.

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

Aquest contracte està finançat per Fons Europeus. El programa RETECH constitueix un dels nous eixos transversals de l'Agenda España Digital 2026 promoguts pel Ministerio de Asuntos Económicos y Transformación Digital, i està alineat amb dues de les principals fites de l'Agenda, com són, liderar la transformació digital de manera inclusiva i sostenible i focalitzar els esforços de digitalització en

sectors econòmics clau. L'objectiu del Programa RETECH és impulsar xarxes territorials d'especialització tecnològica, articulant projectes regionals que s'orientin a la transformació i especialització digital, assegurant la coordinació, la col·laboració i la complementarietat.

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

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

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

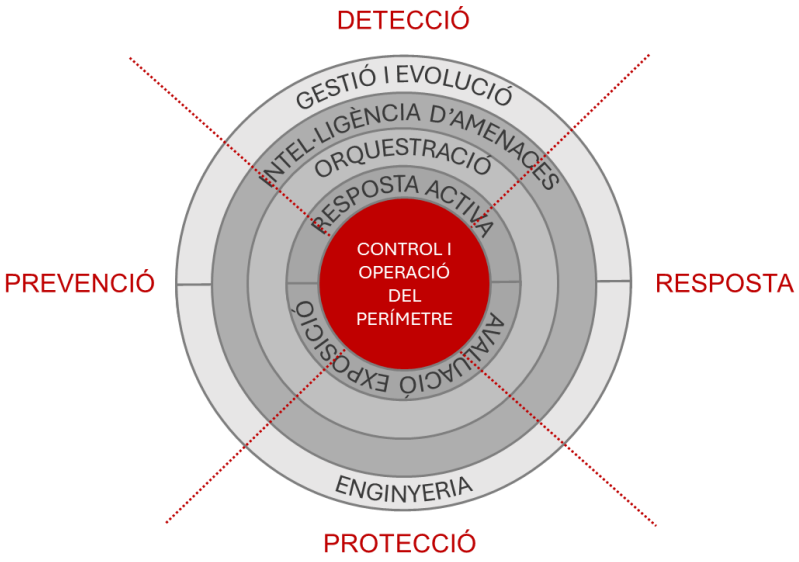
Avui en dia l'Agència té les següents funcions:

- **Gerència** s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació, la gestió de personal, la seguretat corporativa i la captació i gestió de fons que fomenta l'atracció de fons i gestions administratives ó la internacionalització de l'entitat.
- **Operacions** du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció i resposta de seguretat en la seva vessant més operativa (coneguda com SOC/CERT).
- **Desenvolupament d'Estratègia d'Àmbits** (DEA) 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 de Competència i Innovació** en Ciberseguretat (CCI) s'ocupa de la coordinació, cohesió i capacitat de l'ecosistema de Ciberseguretat de Catalunya, recolza el coneixement, sensibilització i conscienciació, i la innovació com a palanca de transformació i creixement del sector.
- **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.

1.2 Funcions del SOC/CERT

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.



Estructura funcional actual del SOC/CERT

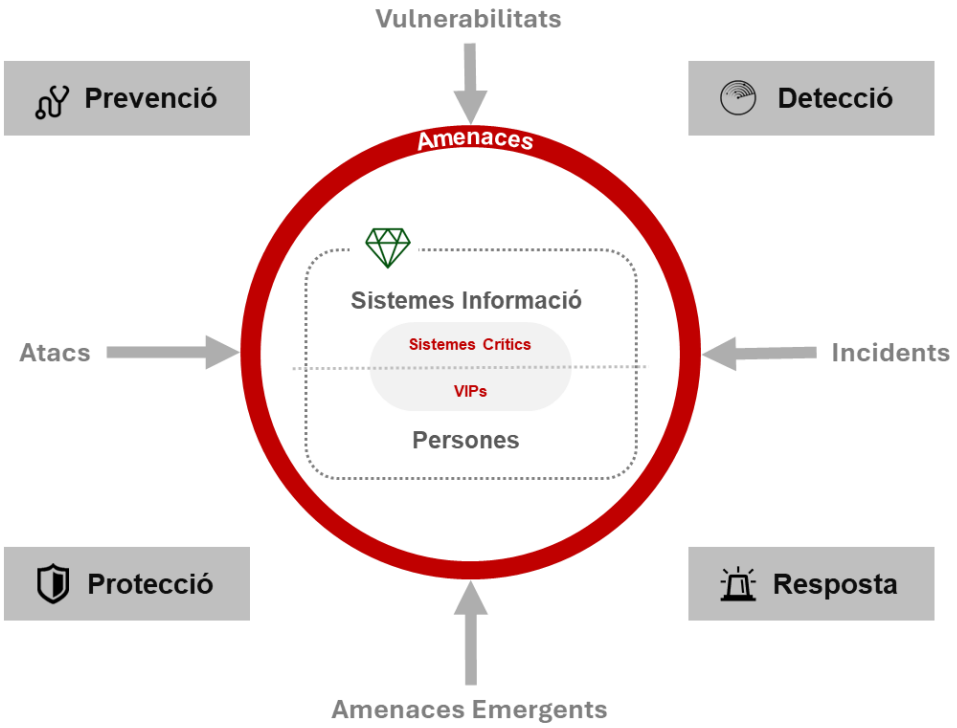
La primera funció és la de **Control i Operació del Perímetre** (COP), que dona resposta a la operació de perímetres dels eixos de detecció, prevenció protecció i resposta. Aquesta funció correspon a tasques relatives a la gestió del cicle de vida dels esdeveniments, vulnerabilitats, amenaces i atacs 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.

La funció de "**Avaluació d'Exposició**" (AVX) dona 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, a més a més s'encarrega de tenir controlada l'exposició de tot l'àmbit. Els serveis objecte de la present licitació s'emmarquen precisament dins d'aquesta funció.

Tot i l'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. Addicionalment, aquesta mateixa funció de manera proactiva i transversal complementa a la d'AVX i realitza cerca d'amenaces '*huntings*' per identificar possibles incidents i altres punts de millora.

Al voltant de les funcions més operatives del SOC/CERT es desplega l'activitat 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.



Plantejament "Threat-Centric"

Justament per sobre de l'Orquestració Operativa, es desplega la funció d'**Intel·ligència d'Amenaces** (IOP), 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 del marc de treball MITRE ATT&CK i també es realitza una tasca analítica de l'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, 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.

2 Descripció dels serveis objecte de la contractació basada.

2.1 Context dels serveis objecte del contracte.

El servei objecte del contracte en aquest plec està contextualitzat en l'expedient AM.02.2024 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.

Concretament s'emmarca en el "Lot 5: Anàlisi tècnic de seguretat".

Dins d'aquest lot s'inclouen, tal i com indica el Plec de Clàusules Tècniques de l'Acord Marc de referència, el suport en les tasques de 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, per tal de conèixer l'impacte que tindrien les diferents amenaces sobre l'àmbit d'actuació fixat en el contracte basat, així com tenir exhaustivament identificada l'exposició de l'àmbit per poder ajudar a identificar o prevenir amenaces.

En general, i a mode de resum, l'Agència busca satisfer son les següents capacitats:

- Obtenir el coneixement del context de negoci, tecnològic i de funcions i serveis de ciberseguretat de les entitats.
- Identificar de manera exhaustiva el grau d'exposició dels diferents actius que composen l'àmbit d'actuació a les principals ciberamenaces del sector.
- Detectar noves exposicions de l'abast de forma precoç, per poder aplicar mesures mitigadores abans de patir atacs.
- Establir el model de relació amb els serveis de l'Agència.
- Garantir l'assegurament de la qualitat dels productes generats i fer una correcta gestió i seguiment del servei.
- Evolució i millora del servei durant la vigència del contracte.
- Retenció del coneixement, així com independització de les persones.

Per fer-ho, en els propers apartats d'aquest Plec Tècnic, s'inclou detall addicional dels serveis a licitar què permetrien assolir les capacitats descrites anteriorment.

2.2 Serveis d'Avaluació de l'Exposició

2.2.1 Objecte i abast dels serveis.

L'objecte de la present licitació és la contractació de les tasques de suport a la gestió i operativa de la funció d'Avaluació de l'Exposició de l'Agència en l'àmbit dels Sistemes d'Informació Crítics (en endavant SICs) de la Generalitat de Catalunya, on aquesta funció s'encarrega de manera simplificada d'identificar i descriure el grau d'exposició a les amenaces d'un conjunt d'actius i col·laborar en l'aplicació de les mesures requerides per reduir dita exposició mitjançant exercicis específics d'anàlisi de seguretat, proves tècniques i tests de penetració.

La present licitació s'estructura en els lots que s'enumeren tot seguit:

- **Lot 1:** SICs dels departaments de Presidència, Interior i Seguretat Pública i Economia i Finances.
- **Lot 2:** SICs dels departaments de la Generalitat de Catalunya no inclosos en cap dels lots anteriorment descrits.

A efectes de claredat, tots els següent apartats apliquen de la mateixa manera als diferents lots identificats, evitant reproduir-los idènticament per cadascun d'ells. No obstant això, en cas de que la informació d'un apartat sigui diferent i específica per a cada lot, el redactat de la licitació ja fa referència explícita a aquesta diferenciació.

2.2.2 Objectius del servei

Els objectius que s'espera assolir amb la prestació del servei són:

- **Calcular el grau d'exposició** dels actius que composen l'àmbit d'actuació definit pel contracte basat, d'acord amb els models i les metodologies acordats amb l'Agència. Aquest càlcul ha de permetre, en definitiva, estimar la probabilitat de que les principals ciberamenaces en seguiment per part de l'Agència, acabin generant algun tipus d'afectació negativa contra els actius avaluats.
- Composició exhaustiva i manteniment de la **superficie d'atac** de l'àmbit d'actuació.
- Contribuir de manera determinant a la **reducció del grau d'exposició** dels actius avaluats, mitjançant la col·laboració amb altres equips durant la implementació de les mesures de mitigació necessàries.
- **Estandardització i normalització del model d'avaluació** del grau d'exposició de l'Agència per tot l'àmbit fixat al contrat basat.

2.2.3 Activitats i funcionalitats

Les activitats i funcions que s'esperen d'aquest servei són:

- **Execució de proves tècniques** de seguretat per la identificació de febleses de seguretat que permetin determinar de forma objectiva el nivell d'exposició dels diferents actius, a les principals ciberamenaces actives a l'àmbit, prenent com a base la informació d'intel·ligència d'amenaces proporcionada per l'Agència, i valorant les mesures de prevenció, protecció i detecció disponibles en les entitats.
- **Preparació i planificació preliminar** de l'anàlisi i proves tècniques, de manera coordinada amb altres possibles serveis de l'Agència involucrats i les pròpies entitats.
- Realització d'escanejos i proves tècniques de forma sistemàtica per **identificar de manera exhaustiva totes les exposicions** dels sistemes i aplicacions. L'objectiu és detectar noves vulnerabilitats i superfícies d'exposició de manera precoç, permetent així la implementació de mesures mitigadores abans que puguin ser explotades en un atac.
- Reconeixement, avaluació i control de **tota la superfície d'atac** de l'àmbit d'actuació fixat en el contracte basat.

- **Compartició o registre de la informació** de context recollida en els repositoris de dades que determini l'Agència per assegurar la disposició d'aquesta per la resta de funcions que puguin requerir-la.
- Generació dels **informes de diagnòstic i lliurables relacionats**, corresponents als actius avaluats, amb la visió consolidada del grau d'exposició a les amenaces.
- Col·laboració activa en la proposta, disseny i la implementació de mesures que permetin **reduir activament la exposició** dels actius avaluats, conjuntament amb d'altres equips de l'Agència, com la funció de Control i Operació del Perímetre o també els responsables dels propis actius de l'àmbit.
- **Presentació de resultats** en representació de l'Agència als responsables dels àmbits avaluats, elaborant el material de suport necessari en els formats acordats prèviament amb l'Agència.
- Disseny de la **planificació de missions d'avaluació**, de manera acordada i conjunta amb l'Agència.
- En els casos on sigui viable, contribució a **l'ecosistema tecnològic i documental** de la funció per poder industrialitzar l'execució de les seves tasques, de manera efectiva i eficient.
- **Coordinació** amb la rest del SOC/CERT i d'altres actors rellevants, per garantir una integració operativa complerta i una prestació del servei autosuficient i alineada amb les necessitats de la funció d'Avaluació de l'Exposició.

2.2.4 Industrialització del servei

Addicionalment a tot l'anterior, el servei objecte del contracte hauria de buscar, contínuament, la industrialització o automatització de les seves funcions per tal d'optimitzar la dedicació dels recursos (humans i tècnics) i augmentar l'eficiència del servei.

En un entorn tant gran com l'àmbit que gestiona l'Agència de Ciberseguretat de Catalunya, es requereix un alt nivell d'industrialització, automatització i normalització de processos. Aquesta industrialització pot ser aplicable a diferents processos, com ara l'execució d'anàlisis tècniques com la documentació de les troballes identificades.

Per la maduració i la industrialització del servei, qualsevol acció, procés o tasca pot ser susceptible de ser industrialitzat. És a dir, en el procés de disseny i desplegament ha de tenir-se en compte aquest objectiu, per la qual cosa haurà de seguir els criteris següents:

- Eficient, en recursos i eines.
- Eficaç, en resultats ràpids, tangibles i avaluables.
- Susceptible de millora contínua.
- Amb relacions d'entrades i sortides i sinèrgies amb la resta de processos.

Per tant, s'han de tenir en consideració aquests criteris a l'hora de definir i pensar en els serveis, processos, procediments i eines, i per tant, s'evitaran propostes de serveis que exigeixin:

- Processos que consumeixin grans esforços de recursos.
- Eines amb baix retorn, tant d'eficiència com d'eficàcia.

- Processos monolítics i aïllats, que no puguin revertir en millores d'altres processos i serveis.
- Coneixements tancats, que no comuniquin i que impedeixen el creixement de l'organització.

Aquest interès per la industrialització de les activitats és un dels eixos d'aquest plec: els clients de l'Agència estan vivint processos de transformació molt actius, el nombre i complexitat de sistemes d'informació i d'elements a protegir creix de manera contínua i les ciberamenaces a les que estan exposats són cada vegada més complexes; tot això fa que el volum de demanda pe l'Agència sigui creixent i la industrialització dels serveis ha de dotar a l'organisme de mecanismes que permetin assumir aquesta demanda amb els mateixos recursos assegurant la seva sostenibilitat i augmentant la seva eficiència.

2.2.5 Lliurables del servei

El model de prestació del servei haurà de contemplar la definició, els continguts i la periodicitat dels lliurables del servei. Entre els lliurables es poden considerar productes que inclouen resums de l'activitat dels serveis periòdicament, 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. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència.

Durant la prestació de servei l'empresa adjudicatària ha de generar i entregar de manera obligatòria els següents lliurables:

Document	Descripció	Periodicitat
Informe d'Avaluació d'Exposició	Informe generat íntegrament pel servei d'avaluació de l'exposició on s'avalua el grau de l'exposició dels actius que composen l'àmbit d'actuació.	Un per avaluació
Bitàcola d'activitat	Descripció detallada de les accions executades durant un exercici d'avaluació.	Una per avaluació
Avís Primerenc	Si durant un exercici d'avaluació s'arriba a identificar vulnerabilitat extremadament crítica, es procedirà a generar una comunicació formal cap a l'àmbit responsable de manera excepcional i fora de cicle.	Puntual
Presentació de resultats	Presentació de resultats en format diapositives, segons models disponibles per part de l'Agència.	Un per avaluació
Documents de treball per valorar el nivell d'exposició a les amenaces	Formularis de treball, a partir de plantilla de l'Agència, que permeten calcular de manera aproximada i objectiva, el grau d'exposició d'un conjunt d'actius davants les principals ciberamenaces i les seves capacitats.	Un per avaluació
Informe d'incidència	Davant una incidència generada com a conseqüència de l'activitat d'una missió d'avaluació, s'haurà de lliurar de manera immediata un informe explicatiu on es detalli la casuística de la situació identificada.	Puntual
Informes de seguiment	Informes de seguiment periòdics de l'estat de les tasques, incloent la planificació, avenços, possibles desviacions, i riscos observats durant el transcurs de totes les activitats.	Mensual

La relació de lliurables de la funció d'Avaluació de l'Exposició, la seva periodicitat i la seva pròpia estructura i continguts podran canviar amb el temps i durant el període d'execució dels serveis que es liciten, d'acord als requisits definits per l'Agència de Ciberseguretat. Els canvis s'acordaran entre

l'adjudicatari i la pròpia Agència de Ciberseguretat, garantint no generar un impacte greu en cap de les dues parts. En aquest sentit també s'haurà de considerar la petició sota demanda d'informes concrets per part de l'Agència.

2.2.6 Mètriques i indicadors del servei

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar en la prestació del servei. L'Agència es reserva el dret d'adaptar aquest llistat de mètriques de manera acordada amb l'adjudicatari.

Indicador	Descripció
Activitat Gestionada	Control del nombre de peticions gestionades pel servei, incloent la seva tipologia i estat.
Missions d'avaluació	Nombre d'exercicis completats pel servei.
Millores aplicades	Nombre i tipus de millores implementades com a conseqüència de les missions d'avaluació.
Reducció de l'Exposició	Rati de millora del grau d'exposició generada com a conseqüència de les missions d'avaluació.
Vulnerabilitats identificades	Nombre de vulnerabilitats identificades de manera agregada i classificada segons tipus i criticitat.
Capacitats d'amenaces avaluades	Nombre de capacitats identificades per la funció d'Intel·ligència Operativa com a rellevants, que han sigut avaluades durant les missions. El diferents tipus de capacitats poden ser, per exemple: tècniques ATT&CK, eines, CVEs o malware.
Avisos primerencs	Nombre d'avisos primerencs lliurats i mètriques relacionades, com ara: temps d'emissió, temps de resolució, etc.
Incidències generades	Nombre d'incidències generades

2.3 Característiques del servei

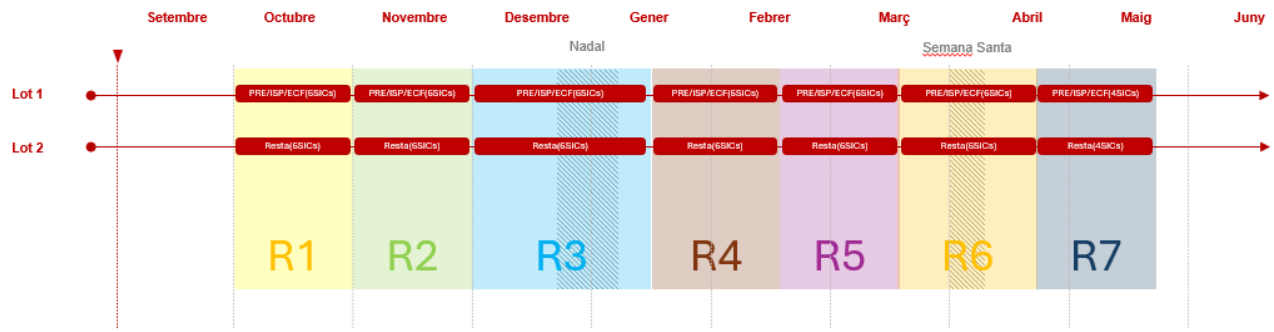
De tot el que s'ha exposat prèviament es pot observar com, en l'execució del contracte han de tenir en compte els següents elements:

- Les activitats es duran a terme seguint les directrius, eines i formats establerts per l'Agència.
- L'avaluació del grau d'exposició a les ciberamenaces haurà d'aportar una visió unificada. homogènia i íntegra, com a resultat de l'activitat executada. Serà imprescindible, per tant, que els membres de l'equip de diagnòstic de cada entitat cooperin i treballin des del primer moment en equip per elaborar i traslladar a l'Agència i posteriorment als responsables dels actius avaluats un relat únic.
- La direcció i supervisió dels equips de treball, així com el control de la qualitat de l'activitat desenvolupada i dels productes resultants formaran part intrínseca de les funcions del servei.

2.3.1 Planificació

- L'Agència juntament amb el Centre de Telecomunicacions i Tecnologies de la Informació (en endavant CTTI) i els propis Departaments de la Generalitat de Catalunya determinaran la planificació i la distribució mensual d'entitats a avaluar, respectant sempre els límits temporals definits pel fons.
- L'execució de totes les tasques i emissió de resultats ha d'estar finalitzada **abans del 30 de Juny de 2026**. Per poder complir amb aquesta data s'estima estrictament necessari avaluar **6 actius alhora** cada mes per part de **cada lot**.
- Cada agrupació d'anàlisis executades en paral·lel durant un mes es considera una ronda d'avaluació.
- Es planteja inicialment un total de **7 rondes seqüencials** per tal de poder avaluar tots els actius inclosos dins l'àmbit d'actuació. La primera ronda s'iniciarà aproximadament durant el mes d'Octubre de 2026.
- Caldrà presentar els resultats de cada avaluació als responsables de l'actiu avaluat en finalitzar cada ronda.
- La planificació de les reunions de kickoff, punt de control i l'entrega de lliurables serà acordada prèviament amb l'Agència. Tanmateix, les ofertes hauran de detallar una proposta de planificació de totes les avaluacions plantejades, observant els requeriments descrits a la definició del plec.
- L'empresa contractista ha d'estar localitzable en tot moment durant les proves d'intrusió per atendre possibles incidències derivades de la seva execució.

Calendari general estimat (exemple a nivell il·lustratiu)



En cas que l'inici del contracte sigui anterior al previst, aquest calendari s'adaptarà a les noves necessitats. Igualment, si l'adjudicació es produeix amb retard, serà necessari reprogramar el calendari per tal de garantir el correcte compliment dels terminis d'execució del contracte.

2.3.2 Volumetria

El nombre de SICs a avaluar per cadascun dels lots que composen la present l'objecte del contrctae queda descrit a continuació:

- **Lot 1:** **40 SICs** dels departaments de Presidència, Interior i Seguretat Pública i Economia i Finances.
- **Lot 2:** **40 SICs** dels departaments de la Generalitat de Catalunya no inclosos en cap dels lots anteriorment descrits.

3 Condicions d'execució del servei

3.1 Horaris

El servei s'haurà de prestar d'acord amb els horaris de prestació dels serveis de l'Agència, **8x5 en horari de dies laborables**. Es considera horari de dies laborables els dies que siguin laborables al centre de treball de l'Hospitalet de Llobregat amb prestació **de 8:00h a 20:00h**.

A petició expressa de l'Agència, es podria demanar la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

Si durant l'execució del contracte l'Agència o l'adjudicatari detecten la necessitat de modificar l'horari del servei o equip descrit en aquest plec, l'Agència i l'adjudicatari consensuaran de forma conjunta la modificació, essent l'Agència qui finalment designi l'horari de prestació que s'adeqüi a les necessitats pròpies i que no perjudiqui de forma excessiva a l'adjudicatari.

3.2 Localització física.

Inicialment, els equips prestataris dels serveis estaran ubicats físicament a les oficines de l'adjudicatari o en alguna altra que ambdues parts acordin, atenent sempre a la seguretat de la informació gestionada pel servei. Tot i això, l'Agència considera que l'adjudicatari, en coordinació amb la Direcció de l'àrea de l'Agència, podria arribar a prestar/executar fins al 75% de les tasques/projectes/serveis amb recursos ubicats a les instal·lacions de l'Agència de Ciberseguretat a l'Hospitalet de Llobregat.

Addicionalment, s'ha de contemplar la possibilitat que part d'aquests serveis requereixin del desplaçament dels professionals a les instal·lacions dels clients de l'Agència que poden estar ubicades a qualsevol part del territori de Catalunya.

Al llarg del contracte es podria requerir un canvi en la ubicació dels professionals, d'acord amb les necessitats dels serveis i l'organització d'equips de treball. En cap cas la ubicació dels professionals suposarà un increment dels costos vinculats a la prestació dels serveis.

3.3 Equip de treball

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

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

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.
- Habilitat per identificar, analitzar i resoldre problemes.
- 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.

3.3.1 Líder Tècnic

Amb independència del model organitzatiu proposat, l'adjudicatari haurà de assignar a un dels perfils identificats el rol de **Líder Tècnic**. Aquest perfil, en base al model de relació de l'Agència, es coordinarà amb els responsables del servei per part de l'Agència **com a punt de contacte principal**, per tal de garantir la correcta execució de les capes de gestió, administració i servei. A aquest efecte, ha de responsabilitzar-se de que els següents punts s'executen per part del servei de manera correcta i continua:

- Coordinació amb la resta d'àrees i equips de l'Agència.
- Generació, implementació i càlcul de les mètriques i els indicadors del servei.
- Lideratge dels aspectes de ciberseguretat recollits en l'àmbit d'actuació del servei en els diferents comitès de seguiment/crisis o problemes endegats per l'Agència o CTTI.
- Gestió i control de la informació com procediments i instruccions operatives.
- Definició, millora i manteniment de procediments i instruccions operatives.
- Generació d'informes referents a incidències de servei, actes, informes executius, informes de resultats o informes de situació, entre d'altres, assegurant sempre la qualitat tècnica i executiva dels informes.
- Integració de l'operativa amb tercers: equips externs i interns o el propi negoci per exemple.
- Suport a la resolució de conflictes i incidències operatives.
- Pla de transformació i detecció d'oportunitats de millora.
- Consolidar i aportar a l'Agència les informacions objectives i subjectives que permetin a la Direcció la presa de decisions operatives, tàctiques i estratègiques relacionades amb el contracte.
- Assegurament de la qualitat del servei prestat i dels lliurables generats (Quality Assurance).
- Gestió de riscos operatius del servei.

3.3.2 Estructura

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

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

L'execució de tots els serveis plantejats s'ha de completar abans del **30 de Juny de 2026**. En aquest sentit, l'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec queda detallada a continuació, segons els diferents lots plantejats en els propers apartats.

Els requisits identificats s'han d'entendre com a mínims aproximats, podent els licitadors ampliar-los i millorar-los a les seves ofertes.

3.3.2.1 Perfils

A continuació, es detallen els perfils professionals que des de l'Agència s'identifiquen per la disposició dels rols adients per la prestació dels serveis desitjats, deixant a la banda dels licitadors la proposta de desplegament, composició de l'equip, adequació de perfils i dedicació global dels mateixos.

Tots els perfils relacionats en aquest apartat i en l'apartat anterior han d'estar adscrits al contracte. L'empresa adjudicatària ha d'adscriure els perfils necessaris per a la correcta execució del contracte.

Les responsabilitats dels diferents perfils són les següents:

- **Avaluador de l'exposició**: entre d'altres, és responsable d'executar les proves tècniques d'anàlisi, processar els resultats corresponents i calcular el conseqüent grau d'exposició a les principals ciberamenaces segons els model definits per l'Agència. Tanmateix, és responsable d'identificar contramesures que permetin reduir dita exposició i col·laborar amb altres equips per assegurar la seva implementació.
- **Coordinador de missions:** responsable de planificar i coordinar la execució de les diferents missions d'avaluació que s'han d'executar en paral·lel.
- **Tècnic de reducció de l'exposició:** responsable d'identificar, dissenyar i col·laborar en la implementació de mesures que permeten reduir el grau d'exposició a l'amenaça d'actius sota la cobertura d'un perímetre de ciberseguretat. Requereix una col·laboració molt estreta amb la resta d'equips del SOC/CERT i exigeix desenvolupar un coneixement detallat sobre els propis actius i els perímetres desplegats.

Addicionalment, per a cada perfil es llisten els requeriments mínims que haurien de complir les persones que assumeixin aquests rols.

PERFIL	REQUISITS
Avaluador de l'exposició	• Coneixements avançats en anàlisi de resultats de pentesting i vulnerabilitats per tal de conèixer les seves implicacions. • Coneixements avançats de les metodologies d'intrusió / pentest (OSSTM, OWASP, MITRE). • Coneixements avançats dels elements de seguretat de les principals tecnologies de cloud computing. • Alt grau de coneixement i experiència en tècnica operativa de Sistemes d'Informació heterogenis, xarxes, softwares, protocols de comunicacions, etc. • 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

PERFIL	REQUISITS
	en protocols, programari maliciós, errors d'implementació, debilitats de configuració, errors o indiferència dels usuaris, entre d'altres. • Certificacions desitjables: OSCP o GPEN o GWAPT
Tècnic de reducció de l'exposició	• Coneixements avançats en anàlisi de resultats de pentesting i vulnerabilitats per tal de conèixer les seves implicacions. • Coneixements avançats de les metodologies d'intrusió / pentest (OSSTM, OWASP, MITRE). • Coneixements avançats dels elements de seguretat de les principals tecnologies de cloud computing. • Alt grau de coneixement i experiència en tècnica operativa de Sistemes d'Informació heterogenis, xarxes, softwares, protocols de comunicacions, etc. • Coneixement d'anàlisi d'alertes SOC i tècniques de detecció i protecció.
Coordinador de missions	• Capacitat d'abstracció i síntesi per tal d'obtenir resultats concisos, generacions de plans d'acció i presentació de resultats. • Coneixements en gestió d'equips i definició de procediments per la realització d'escanejos i test de penetració. • Capacitat de govern, preparació, coordinació gestió de les proves d'avaluació en els diferents àmbits, així com la notificació i resolució de problemes. • Coneixements en metodologies i eines per a la realització d'anàlisis de vulnerabilitats i pentesting. • Coneixements en anàlisi de resultats de pentesting i vulnerabilitats per tal de conèixer les seves implicacions. • Coneixements avançats de les metodologies d'intrusió / pentest (OSSTM, OWASP, MITRE).

S'entén que aquests perfils es corresponen amb els rols que, des de l'Agència, s'identifiquen per la prestació d'aquest servei, deixant a la banda dels licitadors la proposta de desplegament, composició de l'equip, adequació de perfils i dedicació global dels mateixos.

3.3.2.2 Lot 1

A continuació s'inclou l'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats pel Lot 1:

Perfil	Hores mínimes
Avaluador de l'exposició	**8448**
Coordinador de missions	**1584**

Tècnic reducció d'exposició	**1584**

3.3.2.3 Lot 2

A continuació s'inclou l'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats pel Lot 2:

Perfil	Hores mínimes
Avaluador de l'exposició	**8448**
Coordinador de missions	**1584**
Tècnic reducció d'exposició	**1584**

3.4 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte basat el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies laborables a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència a l'empresa adjudicatària del contracte basat. L'adjudicatari haurà de presentar en un termini màxim de 10 dies laborables a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució. Si l'objecte del contracte basat ho requereix, aquest aspecte es podrà concretar en aquest.

3.5 Control de rotació

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

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

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

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

3.6 Eines i equipament per a la prestació de serveis.

Les principals eines requerides (gestió d'esdeveniments, alertes, sistema de registre, anàlisi de codi, web i infraestructura...) per la prestació del servei seran proporcionades per l'Agència. L'Adjudicatari haurà de fer servir aquestes eines, no podent extreure informació fora de l'àmbit d'actuació per la seva manipulació o explotació sense autorització prèvia de l'Agència.

Quan l'adjudicatari es trobi en les instal·lacions de l'Agència, proveirà a les persones que prestin els serveis:

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l'Agència.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides l'Agència.
- Telefonia fixa a les instal·lacions del servei.
- Telefonia mòbil per donar cobertura als serveis de guàrdia.
- Accés a Internet a través de la xarxa d'àrea local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.

L'Agència no proveirà:

- Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina ni tampoc ordinadors portàtils amb el programari habitual de l'Agència.
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.
- Accés a Internet via GPRS, UMTS.
- Cap altre recurs no especificat explícitament.

En conseqüència, els adjudicataris hauran de:

- Subministrar tots elements de maquinari, programari i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments de l'objecte del contracte. Aquests elements seran *d'ús exclusiu* pels serveis prestats a l'Agència i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.
- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.
- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip de Mitjans Tècnics de l'Agència.

L'Agència es troba en un procés de revisió i millora contínua que pot implicar la realització de canvis importants en el referent a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei.

Per aquest motiu és imprescindible que l'adjudicatari tingui presents les següents consideracions en el referent a les eines de gestió durant l'execució del contracte.

- L'Agència decidirà la utilització de qualsevol tecnologia nova o evolució de les existents, relacionades amb la prestació del servei.
- L'Agència decidirà la forma d'implantar qualsevol d'aquests nous sistemes, planificar els projectes corresponents i el seu calendari, així com la transició des dels sistemes existents cap als nous.
- Els adjudicataris es comprometen a assumir i adaptar-se a aquestes noves tecnologies i sistemes per donar el servei de suport, així com participar activament en el procés de transició, formant i preparant el seu personal en aquestes noves tecnologies i sistemes implantats sense cost addicional per l'Agència.

3.7 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions 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 l'empresa adjudicatària registri tot el coneixement que disposi i es generi en la contractació basada que derivi del present contracte basat d'acord amb les directrius del CIC4Cyber.

A tal efecte, l'adjudicatària haurà de mantenir aquest coneixement actualitzat i accessible per a l'organització, havent de proporcionar una descripció detallada del coneixement que es disposi i es generi al servei ofert, i tenint, per part de l'organització, accés a aquest coneixement en qualsevol moment.

3.8 Seguretat Corporativa

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

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

- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (ENS, LOPDGDD, GDPR, LSSI, etc.).

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

3.9 Control de Gestió

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

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

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

3.10 Documentació.

L'Agència és el propietari de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris i el seu personal i subcontractats que destini a l'execució dels serveis.

L'adjudicatari s'encarregarà de disposar de totes les autoritzacions i permisos necessaris per tal de poder donar compliment a aquesta previsió, essent responsabilitat de l'adjudicatari qualsevol pagament o reclamació relativa a aquesta manca d'autoritzacions.

Els responsable de servei de l'Agència serà els responsable de la validació i aprovació dels documents elaborats pel personal de l'adjudicatari. En cas que la qualitat dels documents sigui molt baixa o de manera recurrent i/o perllongada en el temps de prestació dels serveis no assoleixi els nivells requerits s'aplicaran les penalitzacions establertes en el contracte.

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

3.11 Contingència

l'Adjudicatari haurà de proveir un pla de contingència, en cas de desastre de les instal·lacions principals, en unes instal·lacions alternatives (centre de gestió secundari), que inclouran:

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

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

3.12 Metodologia, estàndards i lliurables

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

3.13 Seguretat

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

3.13.1 Deure de confidencialitat

Tot el personal de l'empresa adjudicatària així com els possibles subcontractistes han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat s'haurà de mantenir durant 10 anys, o el que s'especifiqui en el contracte basat, des de que es va tenir coneixement de la informació, excepte en relació a les dades personals a les que accedeixin respecte a les que caldrà mantenir el deure de

confidencialitat de manera indefinida, subsistint inclús quan es finalitzi la relació contractual, segons estableix la Llei Orgànica 3/2018.

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

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

3.13.2 Dades de caràcter personal

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

3.13.3 Compliment del marc legal de ciberseguretat i del marc normatiu intern

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

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

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

3.13.4 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.

3.13.5 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.

3.13.6 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.

3.13.7 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.

3.13.8 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.

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

3.11. Assegurament i control de la qualitat i la millora contínua

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

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

- Anàlisi i avaluació de les dades obtingudes de la mesura del servei, tant de producció i activitat com de gestió de l'incidental i operació.
- Plans de millora del servei orientats a millorar el compliment dels objectius del servei i del negoci.
- Accions per l'assegurament i control de la qualitat (revisions, proves, etc.), amb major rigor, intensitat i profunditat segons la criticitat del projecte/servei/component.
- Accions per reduir el nombre d'incidències, problemes freqüents i el suport.
- Accions per millorar la qualitat percebuda i la satisfacció dels usuaris.
- Accions preventives per la mitigació de riscos, tenint en compte la seva probabilitat i el seu impacte.
- Accions dirigides a millorar la gestió del coneixement i incrementar la usabilitat dels serveis.

- Accions per maximitzar l'eficiència i la sostenibilitat del servei.

3.12. Seguiment del servei

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

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

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

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

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

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

La periodicitat, dates límit de lliurament, canals de transmissió, format exacte i contingut detallat de la informació a elaborar en tots els àmbits del servei, seran definits per l'Agència. L'Agència podrà sol·licitar, durant la vigència del contracte, ampliacions i canvis en el contingut, periodicitat, canals i format de la informació per ajustar-se a les necessitats de seguiment dels serveis.

L'empresa es compromet a automatitzar tot el possible els processos de generació i transmissió de la informació, arribant a la màxima integració possible.

L'empresa es compromet a proporcionar informació veraç i contrastada, i haurà de disposar dels mecanismes necessaris per garantir-ho. L'Agència podrà dur a terme les auditories que consideri necessàries per a la seva verificació, obligant-se l'empresa a participar-hi de manera activa i diligent sense cap cost afegit per a l'Agència.

L'Agència podrà sol·licitar informació de forma immediata i l'empresa hi donarà resposta ràpida fora de la planificació establerta.

3.13. Integració amb altres equips

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

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

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

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

3.14. Compromís amb el talent i la inclusió

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

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

Per deixar palès aquest compromís i voluntat, l'Agència preveu en el present contracte criteris per fomentar la inclusió en la generació de talent i la seva presència en el camp de la Ciberseguretat.

Aquesta mesura reflecteix el compromís amb la igualtat d'oportunitats i la inclusió social, i reconeix el valor afegit que aporta la diversitat funcional en entorns d'alta especialització tècnica. L'activitat de pentesting exigeix capacitats analítiques avançades i una comunicació fluida amb els responsables de les aplicacions avaluades. En aquest context, les persones amb discapacitats diverses poden oferir enfocaments no convencionals que faciliten la detecció de

vulnerabilitats i la generació de solucions innovadores, millorant així la qualitat i eficàcia del servei.