AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Salvador Espriu, 45-51
08908 L'Hospitalet de Llobregat
Tel. 93 557 42 40

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DELS SERVEIS DE SUPORT A LA GOVERNANÇA I EVOLUCIÓ DEL CENTRE D'OPERACIONS DE CIBERSEGURETAT DE CATALUNYA (SOC/CERT).

Exp. CO.07.2022

Índex

1 INTRODUCCIÓ

L'Agència de Ciberseguretat de Catalunya (en endavant, l'"'Agència"), té la necessitat de licitar un conjunt de serveis de suport per a l'execució de les funcions que té recollides a la seva llei de creació i en el desplegament de l'Estratègia de Ciberseguretat del Govern de la Generalitat de Catalunya.

L'Agència, amb aquest encàrrec, assumeix funcions i responsabilitats en l'àmbit de la Ciberseguretat i, en especial, pel que fa al desplegament del servei públic i per garantir una administració cibersegura..

Com a part d'aquesta estratègia, i en consonància amb les necessitats dels seus clients, l'Agència, per portar a terme els seus serveis, i entre ells, l'evolució i la transformació dels serveis de ciberseguretat desenvolupats essencialment en el Centre d'Operacions de Seguretat (SOC) i en el Centre de Resposta d'Incidents de Seguretat (CSIRT o CERT).

1.1 Agència de Ciberseguretat de Catalunya

L'Agència de Ciberseguretat de Catalunya és una entitat de dret públic de l'Administració de la Generalitat de Catalunya que actua amb plena autonomia orgànica i funcional, objectivitat i independència tècnica i professional, i resta adscrita al Departament de Presidència.

L'Agència actua en compliment de la Llei 15/2017 de 25 de juliol de 2017, de l'Agencia de Ciberseguretat de Catalunya.

L'Agència és l'ens públic que succeeix a la Fundació Centre de Seguretat de la Informació de Catalunya (CESICAT), creada l'any 2010, arran de l'acord de govern GOV/50/2009 del 17 de març i se subroga en el convenis i contractes subscrits del CESICAT, amb data 1 de gener de 2020, en virtut d'allò establert a la disposició addicional segona de la Llei 15/2017, del 25 de juliol, de l'Agència de Ciberseguretat de Catalunya, així com el Decret 223/2019, de 29 d'octubre, pel qual s'aproven els Estatuts de l'Agència de Ciberseguretat de Catalunya, que detalla els béns i actius que s'adscriuen a l'Agència, així com els drets i obligacions a què l'Agència se subroga.

Aquest marc legislatiu estableix l'Agència de Ciberseguretat de Catalunya com a entitat encarregada d'executar i de governar les polítiques públiques i l'estratègia en matèria de Ciberseguretat de la Generalitat de Catalunya, sent l'organisme que governa la Ciberseguretat del sector públic a Catalunya.

L'Agència com a encarregada d'establir i de liderar el servei públic de ciberseguretat, 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.

Com a organisme competent en matèria de Ciberseguretat, l'Agència es responsabilitza de l'establiment i el seguiment dels programes d'actuació en matèria de Ciberseguretat, 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.

En les funcions que li són pròpies, l'Agència és l'ens idoni per gestionar les tasques necessàries per assolir aquest objectiu de protecció de la informació i la infraestructura TIC de les institucions i ciutadania de Catalunya i, en especial la del Govern de la Generalitat.

1.1.1 Objectius estratègics

L'Agència de Ciberseguretat de Catalunya neix amb el repte de fer un país cibersegur, i lidera l'Estratègia de Ciberseguretat de la Generalitat de Catalunya 2019-2022, on s'estableix una estratègia operativa de Ciberseguretat basada en la maduresa del govern del risc, fonamentada en l'acció preventiva, en detriment de la reacció com a únic mecanisme de protecció.

L'Agència organitza la seva activitat per mitjà d'un model de governança de la ciberseguretat des d'on es desenvolupen les funcions de protecció, prevenció i resiliència dels sistemes d'informació i les infraestructures TIC de la Generalitat de Catalunya. Aquestes funcions, juntament amb la de governança de la ciberseguretat, conformen la cadena de valor de l'entitat amb una clara orientació a la millora de la maduresa en matèria de ciberseguretat i aportant en tot moment una perspectiva de risc i impacte al negoci.

L'Agència fonamenta la seva activitat estratègica en quatre pilars:

- Desplegament d'un Servei Públic de Ciberseguretat executant polítiques públiques.
- Impuls d'una Cultura de Ciberseguretat que permeti assolir una ciutadania digital plena, conscient i capacitada per a l'ús de les TIC i, en especial, en matèria de ciberseguretat.
- Garantir la Ciberseguretat de l'Administració de la Generalitat de Catalunya i del seu sector públic i de la resta d'entitats i institucions públiques, així com dels ens locals.
- Potencialment del sector econòmic de la ciberseguretat com a sector estratègic, mitjançant polítiques d'innovació, creació de talent i dinamització del sector productiu.

1.2 Grups eventuals interessats

L'Agència de Ciberseguretat de Catalunya, en la seva funció de desenvolupar el servei públic de ciberseguretat necessari per a la protecció del territori de Catalunya davant les amenaces actuals, així com per coordinar la ciberseguretat entre els diferents actors en l'àmbit de Catalunya i garantir la ciberseguretat en els ens locals entre d'altres, cerca establir i impulsar un model de detecció, prevenció, protecció i resposta enfront incidents de ciberseguretat que tinguin lloc arreu del territori. Com a conseqüència té l'encomana de desplegar les seves capacitats a diversos àmbits d'actuació, tots ells inclosos en la següent figura:

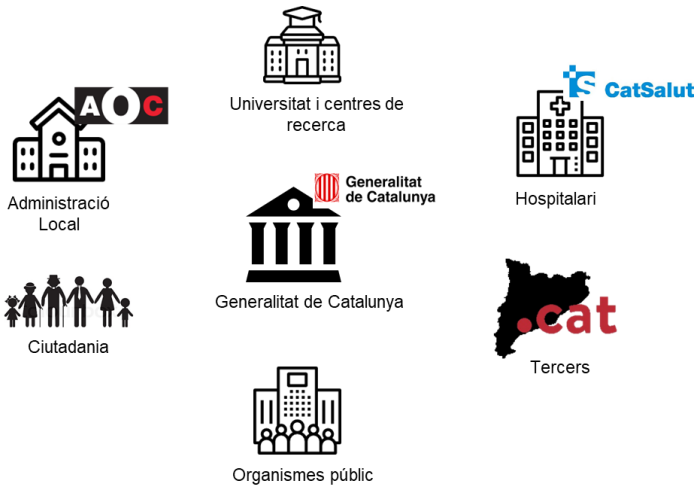

Figura 1. Àmbits d'actuació de l'Agència

1.2.1 L'Agència i les seves àrees

L'Agència està estructurada en àrees dependents de la Direcció General.

Figura 2. Organigrama de l'Agència

Tal i com es mostra en el següent esquema, cadascuna de les 6 àrees de l'Agència es troba formada per diferents línies de servei i serveis que desenvolupen la seva activitat per assolir els objectius i prioritats de l'Agència en matèria de ciberseguretat:

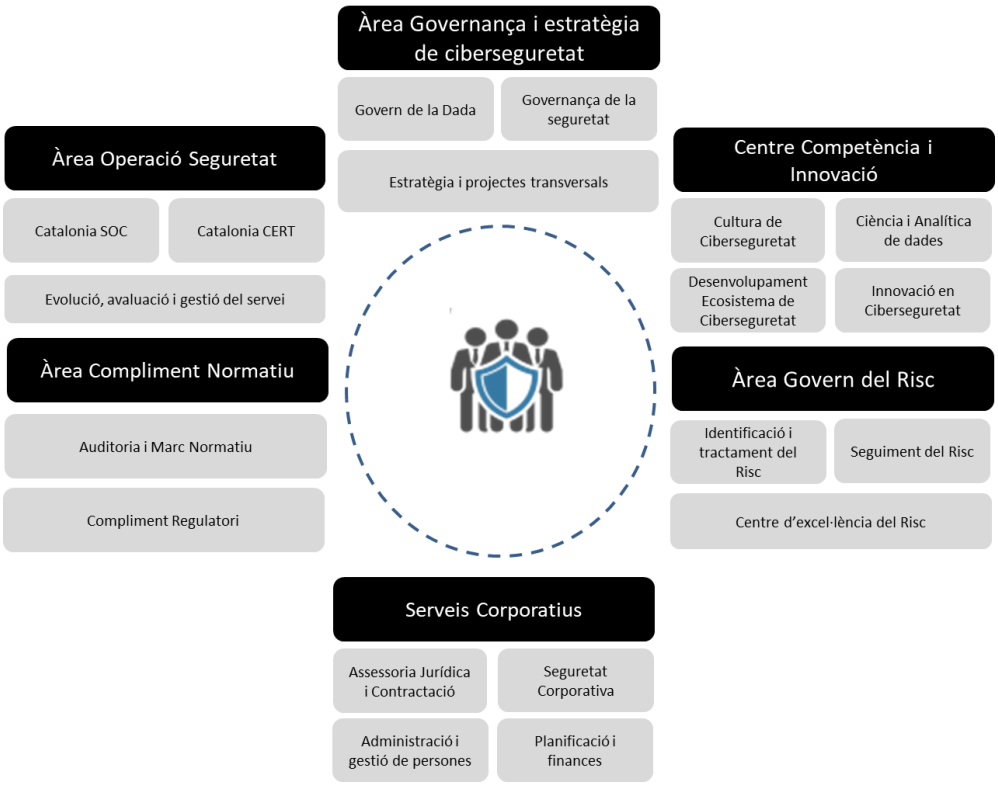

Figura 3. Línies de Servei de l'Agència

1.2.2 Departaments de la Generalitat

Els Departaments de la Generalitat són uns dels clients més destacats de l'Agència de Ciberseguretat. Els diferents Departaments o Conselleries i els seus Ens adscrits conformen la gran part de l'Administració pública de Catalunya.

A més, dins l'àmbit de la Generalitat de Catalunya, es defineixen uns actius prioritaris, nomenats SIC (Sistema d'Informació Crític) i Alt Càrrec (per les persones més rellevants de l'àmbit) en els quals l'Agència de Ciberseguretat de Catalunya ha de garantir especialment la seva seguretat.

1.2.3 Els RSIs

Els Responsables de Seguretat de la Informació (RSI) de l'Agència són una figura que pertany a l'Agència de Ciberseguretat però que es troben organitzativament dins l'estructura dels Departaments de la Generalitat, en relació directa amb les àrees organitzatives, les àrees jurídiques, i, principalment les àrees tecnològiques del departament, i realitzen la funció de responsable de seguretat dels departaments, tenint en compte l'estructura dels mateixos, i amb l'objectiu principal de desplegar el Programa de Seguretat. En aquests rol de gestors de la demanda, la prestació dels serveis aquí descrits proveeixen de les eines i dels mecanismes per portar a terme aquest objectiu cabdal del desplegament del model operatiu.

Els licitadors han d'entendre la figura dels RSI com un CISO departamental.

1.2.4 Centre de Telecomunicacions i Tecnologies de la Informació (CTTI)

El CTTI és l'empresa pública que integra tots els serveis informàtics i de telecomunicacions de la Generalitat de Catalunya, més enllà de proveir solucions transversals i adaptades als Departaments. Els seus objectius inclouen dissenyar, construir, coordinar i desplegar projectes tecnològics, fomentant i incorporant la innovació i la transformació digital.

El CTTI s'encarrega de la gestió, coordinació i modernització tecnològica dels serveis de telecomunicacions i dels sistemes d'informació de la Generalitat, seguint un Pla Global de Transformació (PGT) que té com a objectiu assolir l'estalvi, l'eficiència i la innovació en sis àmbits:

- Lloc de treball
- Aplicacions
- Centres de Processament de Dades
- Telecomunicacions
- Polítiques i estàndards
- Eines de gestió i control de les TIC

Tenint això en compte, el servei objecte de la present licitació ha de ser capaç d'executar els mecanismes adients per tal de fer la integració operativa amb els processos del CTTI (p. ex. obtenció d'informació, resolució d'incidents de ciberseguretat,...), així com canalitzar les comunicacions necessàries per a les vies i eines establertes internament.

1.2.5 Consorci AOC (Administració Oberta de Catalunya)

La missió del Consorci AOC és impulsar la transformació digital de les administracions catalanes, per promoure governs àgils, lògics i col·laboratius.

Els objectius estratègics del Consorci AOC són, fonamentalment, col·laborar amb l'Administració de la Generalitat, els ens locals i, si s'escau, altres organismes públics, per:

- Promoure la interoperabilitat dels sistemes d'informació catalans amb la resta d'administracions.
- Crear i prestar serveis comuns d'administració electrònica.
- Reutilitzar les aplicacions i els serveis d'administració electrònica que es desenvolupin.

- Garantir la identitat i acreditar la voluntat en les actuacions dels ciutadans i el personal del sector públic, així- com la confidencialitat i el no-rebuig en les comunicacions electròniques.

1.2.6 Ciutadania

Com a servei de ciberseguretat públic, l'Agència de Ciberseguretat té la encomana de contribuir a la prevenció de ciberamenaces i a la resposta enfront incidents que puguin afectar a tota la ciutadania del territori. En aquesta línia, el SOC/CERT proveeix el coneixement i els plans d'actuació necessaris per permetre reduir l'afectació de les ciberamenaces que puguin generar un perjudici a la societat de Catalunya i als seus ciutadans.

1.2.7 Universitats, centres de recerca i centres hospitalaris.

L'Agència, en la seva funció de prevenció i resposta davant ciberatacs, inclou dins del seu àmbit d'actuació tant a universitats, instituts universitaris i centres d'investigació públics, com hospitals, consorcis i gerències territorials.

1.2.8 Entitats Locals

L'Agència, en la seva funció de suport i foment de la Ciberseguretat a les administracions locals de Catalunya (Diputacions, Consells Comarcals i Ajuntaments principalment), avalua el nivell de Ciberseguretat de les infraestructures TIC de l'Administració Local per mitjà de convenis de col·laboració, amb l'objectiu de desplegar serveis de Ciberseguretat que la facin més resilient en front d'amenaces cibernètiques.

Alhora, l'Agència actua també en la seva funció de CSIRT de Catalunya en qualitat de Catalonia-CERT®. D'aquesta manera, interactua en l'àmbit de les administracions locals tant a nivell preventiu com també reactiu enfront incidents de Ciberseguretat, prestant alhora un servei d'orientació a aquells organismes que hagin sofert un incident, oferint consells i recomanacions per a la seva prevenció.

1.2.9 Tercers

Aquest àmbit inclou de manera general ens i organitzacions que pertanyen al territori i queden fora de la resta d'àmbits d'actuació. Majorment es tracta d'empreses privades que, no estant per definició incloses dins de les seves competències orgàniques, encara poden aprofitar el valor generat per l'Agència de Ciberseguretat de Catalunya, especialment a l'hora de reforçar les seves pròpies capacitats per prevenir i respondre enfront ciberamenaces. En aquest àmbit, l'Agència de Ciberseguretat, i en concret el SOC/CERT, adopten una posició més orientada a aportar coneixement i acompanyament, si escau, en les tasques de prevenció i resposta.

Per últim, dins del context de l'acord vigent entre l'Agència de Ciberseguretat de Catalunya i la Fundació .CAT, també s'inclouen en aquest àmbit tots els llocs web amb un TLD (*Top Level Domain*) ".cat".

1.3 Modelització de la gestió de la Ciberseguretat de la Generalitat de Catalunya

Degut al model de gestió de les TIC a la Generalitat de Catalunya, amb una alta externalització dels mateixos, el model de gestió de la ciberseguretat de l'Agència s'ha adaptat al mateix, tenint en compte les particularitats inherents a tot model externalitzat, així com al seu govern per part del CTTI, òrgan encarregat de la gestió TIC de la Generalitat.

Com a conseqüència, i seguint al descrit en els punts anteriors, l'Agència desenvolupa un model de Ciberseguretat, i un model de riscos associat, que té en compte:

- L'activitat pròpia de la Generalitat i propi dels seus Departaments.
- El model de gestió TIC externalitzada i dinàmicament canviant.
- Els serveis i objectius de ciberseguretat propis de l'Agència.
- El model operatiu de la ciberseguretat.

En aquest model de ciberseguretat, una peça cabdal és el **programa de seguretat**. L'Agència ha desenvolupat un Programa de seguretat específic per cada Departament de la Generalitat. Aquest Programa és un full de ruta que marca les línies d'activitat i les accions a desplegar en els Departaments de la Generalitat per aconseguir els objectius de ciberseguretat marcats. Per tant, les accions que es despleguen des de l'Agència, sempre estan sota el paraigües d'una acció coordinada i prioritzada. El Responsable de Seguretat de la Informació (RSI) de l'Agència és qui governa la confecció i el desplegament d'aquest programa als Departaments.

La demanda dels serveis objecte d'aquesta licitació amb els Departaments de la Generalitat de Catalunya es canalitza, principalment, mitjançant els programes de seguretat.

Els programes, igual que la resta d'activitats, reflecteixen la cadena de valor de l'Agència.

Figura 4. Cadena de valor de l'Agència

Un altre aspecte molt rellevant que afecta a totes les àrees i serveis de l'Agència és la conceptualització dels objectius estratègics de l'Agència en base a 5 eixos estratègics sobre els quals pivota tota l'activitat i esforços. Aquests eixos estratègics, també reflectits en els programes de seguretat són els que es mostren a continuació:

Figura 5. Eixos estratègics de l'Agència

- **Eix SIC – Sistemes d'Informació Crítics**: té per objectiu garantir la correcta prevenció, protecció, securització i el funcionament segur dels Sistemes d'Informació Crítics dels departaments per tal de reduir els riscos als que puguin estar subjectes els serveis, processos, i dades d'aquests sistemes
- **Eix Persones**: té per objectiu minimitzar els riscos de ciberseguretat als que poden estar sotmeses les eines i els processos de l'entorn tecnològic de treball del personal de la Generalitat de Catalunya, departaments i organismes adscrits, garantint la seva protecció i securització.
- **Eix Cultura de ciberseguretat**: té per objectiu vetllar per una societat digital segura en el conjunt de l'administració de la Generalitat i de la ciutadania. L'assoliment d'aquest objectiu, requereix la promoció del coneixement de ciberseguretat, definint línies d'acció adaptades a les necessitats dels diferents col·lectius.
- **Eix Model de governança**: té per objectiu posar a disposició dels departaments les eines, recursos, processos i metodologia adequats per poder dotar-lo d'un model de governança extensible als organismes adscrits, amb l'objectiu de gestionar els riscos de ciberseguretat.

- **Eix Infraestructures Transversals**: té per objectiu garantir la correcta prevenció, protecció, securització i el funcionament segur de les infraestructures i serveis transversals de la Generalitat de Catalunya i de les administracions locals.

Sobre aquests eixos, l'Agència focalitza la seva activitat per anar assolint els objectius estratègics i operatius fixats. Sobre aquests eixos, els serveis construeixen indicadors que permetin avaluar el grau d'assoliment així com determinar quines són les àrees amb més riscos de ciberseguretat on l'entitat ha de posar més focus.

1.4 Descripció i context dels serveis actuals del SOC/CERT

De totes les àrees que formen l'Agència de Ciberseguretat de Catalunya, l'Àrea d'Operacions s'encarrega d'executar 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.

Aquesta àrea, a la que internament es fa referència com SOC/CERT, s'organitza precisament en tres línies principals de treball:

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

Els serveis objecte de la present licitació 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 la governança, evolució i transformació de les diferents funcions d'operació de la ciberseguretat que composen la funció de SOC/CERT.

1.4.1 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 de la present licitació es relacionaran amb aquestes altres funcions i amb els seus corresponents serveis de suport subjacents.

Figura 6. Funcions i subfuncions actuals del SOC/CERT

1.4.2 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 l'Agència de Ciberseguretat de Catalunya.

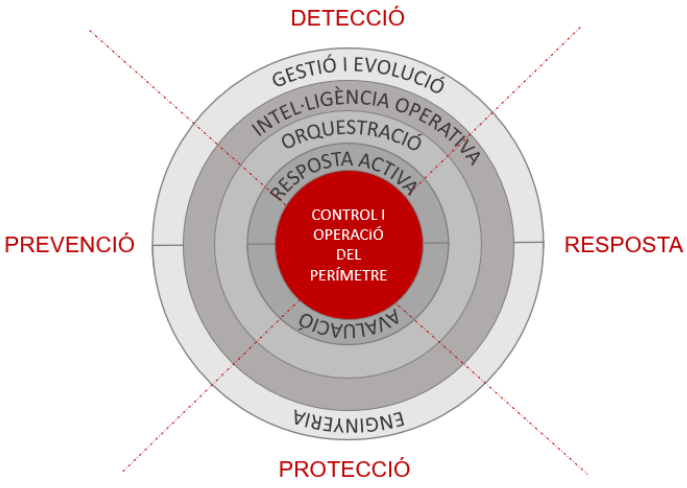

Figura 7. Estructura funcional actual del SOC/CERT

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.

La funció **d'Avaluació Operativa (AOP)** 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.

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, 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.

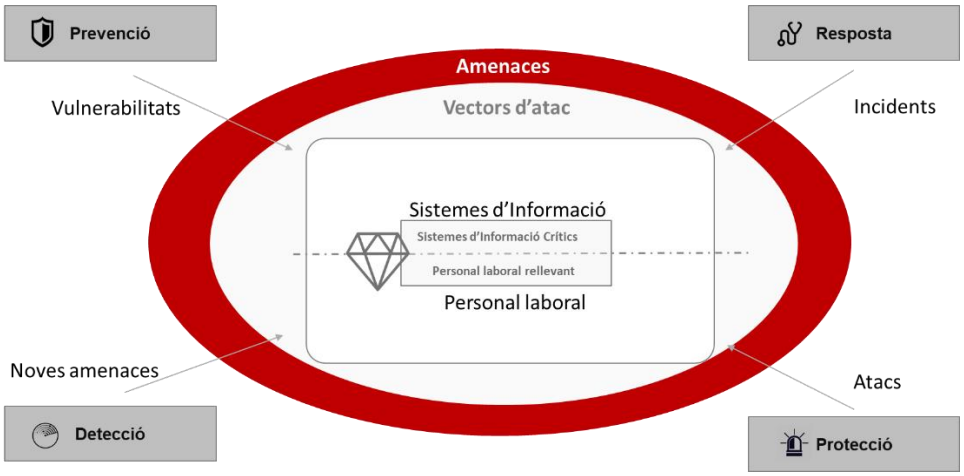

Figura 8. Plantejament "Threat-Centric"

Justament per sobre de l'Orquestració Operativa, es desplega la funció **d'Intel·ligència Operativa (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 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 "**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.

Per últim, i també de manera transversal, la funció de **Desplegament i Enfortiment del Perímetre** 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.

1.4.3 Industrialització de serveis

Durant aquests darrers anys, s'han desplegat diversos serveis i processos de seguretat susceptibles de ser industrialitzats. Després d'una maduresa suficient aquests serveis han de poder entrar en la roda de l'operativa diària amb el mínim esforç i retorn escaient, i amb la voluntat que els recursos s'alliberin pel disseny de nous serveis.

Per la maduració i la industrialització dels serveis, qualsevol servei, subservei o procés del contracte ha de 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

En conseqüència, els serveis objecte d'aquesta licitació han de poder complir amb els objectius d'eficiència operativa i el màxim retorn de les inversions.

Finalment, s'ha de tenir em compte que la industrialització d'una tasca determinada no consisteix obligatòriament en la seva mecanització o automatització; en l'àmbit concret d'aquest plec podem trobar tasques de consultoria en les que la industrialització pot esdevenir-se, a tall d'exemple, en la creació de models, estàndards o documents d'auto avaluació del compliment normatiu.

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 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 SERVEIS DE SUPORT A LA GOVERNANÇA I EVOLUCIÓ DEL CENTRE D'OPERACIONS DE CIBERSEGURETAT DE CATALUNYA.

Tal com s'ha comentat prèviament, una de les funcions transversals del SOC/CERT és la de "Evolució, Avaluació i Gestió del Servei SOC", objecte d'aquesta licitació. Aquesta funció te com a objectiu resoldre activament les necessitats i problemes del SOC/CERT, permetent la seva evolució, 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.

Per donar suport a aquestes funcions més transversals dins del SOC/CERT es defineixen tres lots per segregar responsabilitats dins de la funció:

- **Lot 1**: El servei de suport a l'àrea d'operacions de la seguretat per a la funció de **Governança de l'operació del SOC/CERT**, encarregada de la definició i suport dels serveis necessaris per la execució i coordinació de les diferents tasques operatives associades a la operació del SOC/CERT; així com la determinació dels processos de monitorització i *reporting*, que permetin posar en valor les tasques executades com a part de totes les funcions del SOC/CERT.

- **Lot 2**: El servei de suport a la funció de **Gestió de Projectes i Pla d'Evolució** del servei d'Evolució i transformació del SOC/CERT, té com a objecte principal la identificació, conceptualització i gestió d'iniciatives (tant tecnològiques com organitzatives) que permetin l'evolució del SOC/CERT.

- **Lot 3**: El servei de suport a la funció d'**Arquitectura de seguretat i Evolució de solucions** del servei d'Evolució i transformació del SOC/CERT, té com a objectius principals l'avaluació i disseny de la seguretat dels entorns tecnològics competència de l'Agència, millorar l'eficiència i l'eficàcia dels serveis del SOC/CERT a través de la industrialització i l'automatització dels seus processos i l'evolució de les solucions de Ciberseguretat, donant compliment a les necessitats de transformació i evolució que s'originen dins el SOC/CERT.

Els següents apartats defineixen amb un major grau de detall els serveis de suport objecte d'aquesta licitació i les seves característiques.

2.1 LOT 1: GOVERNANÇA DE L'OPERACIÓ DEL SOC/CERT

L'objecte del Lot 1 es focalitza en la prestació d'un servei de suport a la governança de l'operació del SOC/CERT de l'Agència, sent la seva finalitat principal prestar un servei transversal que permeti la millora de la gestió de les tasques administratives necessàries, així com els processos de monitorització i presentació del valor, que els diferents serveis generen amb la seva activitat.

El servei està composat pels següents àmbits de treball:

- Gestió del Coneixement
- Govern de la operativa del SOC/CERT
- Entrega de Valor

Així mateix, el servei també té fins a 5 principis que regeixen el seu disseny:

- El servei **focalitzarà** la seva capacitat en **governar la coordinació** entre els diferents equips operatius del SOC/CERT, vetllant per l'assoliment conjunt dels objectius estratègics i tàctics de l'Agència.
- En aquesta línia, el servei ha de **garantir que els serveis** del SOC/CERT **disposen d'informació de context de qualitat** per facilitar la gestió i resposta adient a les ciberamenaces.
- De la mateixa manera, el servei ha de desenvolupar els processos oportuns per oferir una **gestió àgil de la demanda** dirigida al SOC/CERT.
- El servei **potenciarà missatges de valor** respecte els resultats de l'activitat operativa de tot el SOC/CERT, alineats amb la seva aportació al negoci i l'eficiència de l'operació de la seguretat.
- El servei ha de ser **autònom** amb capacitat de lideratge i de **defensa dels interessos de l'Agència**.

Finalment, es destaquen els objectius que s'han d'assolir en la prestació del servei, tenint en compte l'orientació cap a resultats que s'espera:

- Situar la funció de "Governança de l'operativa del SOC/CERT" com a referent dins del SOC/CERT i l'Agència per canalitzar qualsevol sol·licitud o petició referent a l'operació de la seguretat.
- Establir els **canals oportuns amb cadascun dels àmbits** per proveir coneixement generat arrel del 100% de l'activitat operativa rellevant.
- Establir els **canals oportuns** amb **cadascuna de les àrees de l'Agència** per disposar i proveir **informació de context** rellevant de les ciberamenaces aplicables en base al coneixement del negoci i l'activitat operativa.

- Definir i documentar els **models de gestió de la demanda** pels **principals tipus de peticions rebudes al SOC/CERT** (serveis inclosos al catàleg de serveis, peticions de CTTI, peticions de tercers...).
- Liderar l'**orquestració dels serveis** per minimitzar el temps màxim per la resolució dels focus operatius gestionats pel SOC/CERT.
- Dotar de la **capacitat de decisió de manera àgil** al SOC/CERT basada en el disseny, suport en la implantació, i millora de quadres de comandament estratègics i tàctics.
- Actualitzar i mantenir **els processos de gestió de la dada** per a la informació operativa més rellevant per al SOC/CERT.
- Garantir la **ciberamenaça com a element vehicular** del 90% de l'activitat operativa del SOC/CERT.

Amb l'objectiu de dur a terme satisfactòriament el servei que dona suport a aquestes subfuncions, els serveis objecte del present lot hauran de desenvolupar, com a mínim, les accions que es detallen en els següents apartats.

2.1.1 Gestió del Coneixement

2.1.1.1 Definició i manteniment del model de dades operatiu i de context

Cal definir i mantenir un model de govern que permeti aconseguir el màxim valor de les dades tractades pel SOC/CERT, donant suport a tots els nivells possibles, des de la presa de decisions a la recerca de noves solucions i models d'operació de la seguretat alineats amb els objectius estratègics de l'Agència.

La definició del model s'ha de dur a terme per permetre respondre a aspectes rellevants sobre la pròpia gestió de la dada i el seu cicle de vida, què com a mínim inclourà les següents tasques::

- Identificació de la informació mínima requerida per garantir una correcta operació de la seguretat dels actius dins de l'abast, procurant estandarditzar la tipologia de dades per tots els actius de les mateixes característiques.
- Classificació i priorització de les dades requerides pel SOC/CERT per acomplir les seves funcions operatives.
- Coordinació amb els equips tècnics corresponents per assegurar que les bases de dades i repositoris del SOC/CERT inclouen tota la informació requerida.
- Identificació de les fonts origen considerades vàlides per la recollida de les dades d'interès i definició dels canals/fluxos/mètodes establerts per actualitzar-la, on les fonts poden ser sistemes d'informació o equips de treball d'alguna de les àrees de l'Agència o de tercers.
- Identificació de responsables o propietaris de la informació de les fonts de dades definides.
- Definició de criteris per al manteniment i conservació de la informació, incloent el període d'actualització, vigència i/o retenció. Aquest criteris hauran de complir els requeriments normatius o legals que puguin limitar o determinar els mètodes de tractament d'acord amb les directrius que marqui l'àrea corresponent de l'Agència (actualment Compliment Normatiu).
- Identificació de les persones, serveis de l'Agència o ens als quals donar accés a la informació, ja sigui de manera directa amb accés als repositoris del SOC/CERT (permisos de lectura o edició, depenent del cas), o compartint amb aquests contingut més estàtic i estructurat (p.ex. Fets rellevants, butlletins, informes mensuals, etc.).

Actualment, l'Agència gestiona un entorn molt complex on conviuen una gran varietat d'entorns tecnològics i usuaris dels sistemes d'informació (Per exemple, només en l'àmbit de la Generalitat de Catalunya l'abast és d'uns aproximadament 2.000

sistemes d'informació, distribuïts en més de 5.000 servidors, i 300.000 usuaris). A la vegada, l'Agència necessita interactuar contínuament amb diferents interlocutors, tant de negoci (departaments i els seus responsables de seguretat - RSIs), com altres àrees de l'Agència, com els diferents ens que composen el sector públic de Catalunya (hospitals, administracions locals, empreses, etc.).

D'igual forma, l'Agència, disposa d'un inventari de solucions de ciberseguretat, que agrupa les diferents solucions de ciberseguretat desplegades tant pels departaments de la Generalitat de Catalunya, com per la pròpia entitat en l'entorn corporatiu de l'Agència, el qual requereix un manteniment i actualització constant.

Per tot plegat, serà objecte del servei licitat implementar els mecanismes necessaris per assegurar que la resta d'equips del SOC/CERT de l'Agència de Ciberseguretat disposin, en tot moment, d'informació complerta i rellevant sobre l'actualitat arreu dels àmbits d'actuació que pugui condicionar les tasques operatives i el seu esdevenir.

Per acomplir l'objecte d'aquest servei de Gestió del Coneixement, es contemplen les següents activitats:

2.1.1.2 Gestió de la informació del context operatiu

- **Identificació i registre de la dada de context**

Amb l'objectiu de poder identificar i poder respondre de manera eficient a qualsevol ciberamenaça que afecti als actius inclosos en l'àmbit de responsabilitat de l'Agència, és primordial que el SOC/CERT disposi del coneixement adient per entendre el context dels mateixos. En aquest sentit, és responsabilitat del servei assegurar que es disposa de la informació necessària i actualitzada, la majoria provinent d'altres àrees de l'Agència, i garantir que aquesta està disponible per la resta de funcions del SOC/CERT.

Així, i entre d'altres, caldrà dur a terme la gestió continuada de la informació mínima i de la seva classificació per cada actiu, ja siguin inventaris de persones (Alts càrrecs, altres empleats dels ens públics) o de sistemes d'informació (crítics i no crítics) dels àmbits d'actuació responsabilitat de l'Agència. Addicionalment, arrel de la relació amb negoci, s'haurà de poder identificar possibles esdeveniments crítics susceptibles de requerir accions especials durant l'operativa dels serveis operatius (per exemple períodes d'eleccions, preinscripcions universitàries, adjudicació de places públiques, etc.), identificar canvis de responsables de seguretat departamentals, etc.

- **Coordinació amb tercers per l'obtenció d'informació de context**

Caldrà generar i automatitzar de la manera més eficient possible la recollida i manteniment de la informació externa prèviament identificada (inventaris i altra informació de context) per assegurar què estiguin actualitzats i siguin consumibles pels serveis operatius del SOC/CERT. Per fer-ho, serà important disposar d'un model de relació establert, tenir capacitat de coordinació amb tercers responsables de les

dades de context, i coordinar els diferents equips involucrats que permetin la ingesta o modificació de dades directament des de les diferents fonts internes dels serveis de l'Agència que contenen aquesta informació.

- **Control de qualitat i manteniment de la informació del context**

Caldrà definir i implementar els processos i controls adients per garantir la qualitat de la informació de context als repositoris del SOC/CERT. En cas de trobar o sospitar que un actiu no està correctament actualitzat i/o no es té visibilitat sobre alguns camps, cal definir clarament el mètode/canal de notificació amb els responsables de la dada i se'ls ha d'avisar per tal que comprovin l'estat de l'actiu i l'actualitzin si és necessari.

2.1.1.3 Gestió de la informació operativa de ciberseguretat

- **Identificació i registre de la dada operativa**

Com a part de l'activitat operativa de les funcions del SOC/CERT aquestes generen gran quantitat d'informació de valor. És responsabilitat d'aquesta funció assegurar que els equips operatius responsables registren adequadament tots els esdeveniments de seguretat produïts i gestionats per la seva part, així com analitzar-los des de un punt de vista més tàctic per identificar possibles tractaments agregats, necessitats de creuament de dades, i en general facilitar el coneixement de la situació de seguretat dels actius en tot moment.

Caldrà dur a terme el seguiment i millora continua del registre de l'activitat operativa de les funcions del SOC/CERT, essent necessari generar la informació diària de l'estat de seguretat dels actius i facilitar que sigui accessible de manera àgil per a les parts que es defineixin.

A tall d'exemple, s'haurà de disposar d'informació mínima de tots els atacs, incidents, amenaces i incidències gestionats pels diferents equips que conformen les funcions del SOC/CERT, permetent identificar criticitat, tipologia, origen, actius afectats, etc.

Caldrà generar i automatitzar els inventaris i la seva informació associada provinent de les diferents eines que continguin informació dels mateixos i la seva activitat operativa relacionada (eina de tiqueting OTRS, INFOSOC, Consoles d'Antivirus, Filtrat de continguts, SIEM, entre d'altres) per tal de que estiguin actualitzats i siguin accessibles per a la resta dels serveis operatius o altres consumidors que es defineixin. Per fer-ho, el servei s'haurà de coordinar amb l'equip intern del SOC d'Evolució de Solucions per garantir la definició d'un model de dades adient i la integració tecnològica adient per mantenir tots els registres necessaris en els repositoris del SOC/CERT.

❖ **Control de qualitat i manteniment de la informació operativa**

Al igual que es farà amb la informació provinent de tercers fora del SOC/CERT, també caldrà definir i implementar els processos i controls adients per garantir la qualitat de la informació generada per la pròpia operativa de les funcions del SOC/CERT i el seu registre als repositoris del SOC/CERT.

En cas de trobar o sospitar que alguna informació no està correctament actualitzada i/o no es té la visibilitat adient que permeti generar valor i transmetre els resultats de les funcions del SOC/CERT, cal definir clarament el mètode/canal de notificació i coordinació amb les funcions responsables i avisar-los per tal que comprovin l'estat de la mateixa i l'actualitzin, en cas de ser necessari.

2.1.2 Govern de l'operativa del SOC/CERT

2.1.2.1 Disseny i manteniment de models de relació interns

Serà funció d'aquest servei la definició dels mecanismes adients que permetin assegurar la correcta comunicació entre els diferents equips operatius del SOC/CERT, així com garantir la compartició d'informació de manera bidireccional amb les parts que s'acordin.

Com a mínim, haurà d'encarregar-se de les següents activitats:

- Identificació de serveis interns o externs del SOC/CERT amb els que interaccionar de manera periòdica per compartir informació operativa o de context.
- Identificació d'aspectes a tractar i informació a compartir amb cadascun dels serveis interns o externs del SOC amb els que s'identifiqui interacció periòdica.
- Determinació dels fluxos i canals de comunicació a utilitzar entre les parts interessades, incloent la formalització d'un model de relació que s'haurà de mantenir actualitzat durant la prestació del servei.

2.1.2.2 Gestió i seguiment de la demanda.

Serà funció administrativa d'aquest lot, la gestió i operació d'un servei de Suport a la Gestió de la Demanda, per tal de donar el suport administratiu a la resta de serveis del SOC/CERT portant a terme activitats com les següents, entre d'altres:

- **Actuar com a punt principal de contacte del SOC/CERT de l'Agència** (correu electrònic, eines de gestió de tiqueting, atenció telefònica) amb els seus clients, i **canalitzar els casos rebuts cap als equips corresponents dins o fora del SOC/CERT**.

- Assegurar la capacitat de **mantenir informats als clients del progrés i estat de situació** de les seves peticions.
- **Canalitzar les principals comunicacions del SOC/CERT cap als seus clients** relacionades amb l'operació de la seguretat i la prestació dels serveis de catàleg (notificació d'intervencions, alertes especials, gestió dels serveis de subscripcions, etc.).
- **Canalitzar les comunicacions entre l'Agència i el seus '*partners*' tecnològics** (CTTI, AOC, IMI, etc.) per a la seva integració operativa, a partir de les eines acordades entre les parts.
- **Fer la gestió dels formularis i el control de la qualitat** de les dades d'entrada als processos de provisió de serveis (peticions, incidències, RFCs, etc.)
- **Actuar com a taula de canvis i incidències** per tal de fer el seguiment per a la resolució de les mateixes.
- **Analitzar de manera recurrent el conjunt de la demanda tractada pels serveis del SOC/CERT** per:
    - Fer seguiment de l'estat de les peticions d'execució de serveis del SOC/CERT per garantir de manera general la prestació de serveis de qualitat.
    - Garantir el correcte compliment dels fluxos definits per la gestió de la demana.
    - Donar suport a la presa de decisions en relació a la seva classificació, priorització.
    - Identificar possibles ineficiències o punts de millora en la gestió de la demanda.
- **Col·laborar en l'estandardització i automatització** de les tasques més repetitives del servei de Suport a la Gestió de la Demanda del SOC/CERT com objectiu del guany d'eficiència dels recursos del servei.

Amb aquestes directrius, l'equip adjudicatari haurà de considerar el desenvolupament de funcions d'administració del servei, tant de l'organització interna, així com de les relacions amb la resta d'equips de l'Agència. Aquestes funcions s'hauran de focalitzar en el suport i l'assessorament a nous projectes i canvis, ajudant amb el seu coneixement, proves i investigació a la transformació de la mateixa Agència.

2.1.2.3 Orquestració operativa

La orquestració operativa és un dels procediments operatius claus del SOC/CERT i té com a objectiu principal **establir els procediments necessaris per garantir la coordinació operativa entre els diferents serveis de l'àrea SOC/CERT i assegurar la consecució dels objectius generals del SOC/CERT**,**i el focus a les tasques de major rellevància global.** En tot cas, ha de garantir la prevenció, protecció, detecció i resposta davant les diferents ciberamenaces que puguin afectar a la Generalitat de Catalunya i altres àmbits d'actuació de l'Agència.

Actualment, la orquestració operativa del SOC/CERT és un procés ja establert, el qual es desenvolupa mitjançant l'execució de reunions diàries les quals són coordinades pel present servei (actualment a les 11:00h i 16:30h). En aquestes reunions hi participen totes les funcions del SOC/CERT, i es determina a la primera de les mateixes els principals focus de treball de l'àrea durant el dia, en funció de les principals ciberamenaces aplicables. A la segona reunió s'analitza tant l'evolució de les tasques que s'han definit dintre dels focus operatius, així com el seu tancament.

Finalment, el resum de les principals tasques executades durant el període són recollits en un document denominat "Fets Rellevants", el qual és distribuït internament a l'Agència.

D'igual forma, l'Orquestració Operativa determina les activitat de focus diari distingint entre 3 àmbits principals:

- **Focus operatiu**. Totes aquelles tasques implicades en l'operativa diària dels serveis del SOC/CERT, dirigides a complir els objectius de l'Agència (gestió i protecció davant atacs, gestió i resposta a incidents, gestió d'amenaces, etc.).
- **Focus Evolutiu**. Totes tasques dirigides a millorar l'eficiència de l'operativa dels serveis i en general millorar la maduresa del SOC/CERT.
- **Focus Incidental**. Totes aquelles tasques dirigides a resoldre incidències identificades sobre les eines què utilitzen els serveis en la seva operativa diària.

Per tot plegat, els principals àmbits a assolir en la funció d'orquestració són:

- **Rol de coordinació entre els serveis operatius.**

El servei licitat s'ha d'encarregar de governar, dirigir i moderar aquestes reunions d'orquestració, vetllant per a que les activitats acordades dirigides a resoldre els diferents focus definits es duen a terme correctament, sense contratemps, i mantenint sempre un alineament i un objectiu comú entre els equips d'operacions.

D'igual forma, serà funció del rol de coordinació el suport a la resolució de conflictes operatius que es puguin donar entre els serveis, vetllant en tot cas pels interessos globals del SOC/CERT.

Addicionalment, s'ha d'encarregar de definir els processos que regiran les relacions entre els equips d'operacions, on es tractaran, per exemple, el canal i la metodologia per realitzar una sol·licitud d'execució d'una operació, la modificació d'una operativa, etc. A la vegada, haurà de vetllar pel correcte desplegament dels procediments establerts, definint els indicadors necessaris per monitoritzar el grau de desplegament.

Com a suport indispensable a aquest rol, es troba la funció d'Intel·ligència Operativa, amb la qual el servei s'haurà de coordinar en tot moment per assegurar que les tasques realitzades pel SOC/CERT són òptimes per prevenir l'amenaça i respondre diligentment als incidents.

- **Generació de procediments i fitxes d'orquestració.**

L'adjudicatari haurà de garantir que cada àrea aporta la informació necessària i de qualitat per omplir les fitxes requerides per a cada focus tractat en la orquestració. Aquestes fitxes són un resum de l'activitat generada i fites planificades-assolides per cada servei en relació a les tasques establertes a cada orquestració. L'adjudicatari podrà proposar nous formats per la realització de la present tasca.

Igualment, serà funció del present servei la definició i formalització dels procediments d'orquestració implementats durant la prestació del servei.

- **Visió general dels serveis d'operacions i proposta de millores.**

La funció d'Orquestració Operativa ha de treballar per tenir una visió general de l'operativa dels serveis d'operacions i ha de proposar millores, tant per al seu propi servei com per als altres, per tal d'arribar a la màxima cohesió, eficàcia i precisió en l'operativa global del SOC/CERT.

- **Alineament en el desplegament dels objectius tàctics i operatius.**

A la vegada, serà fonamental l'alineament de la funció d'Orquestració Operativa amb els objectius tant tàctics com operatius establerts per cada servei. Per aquest fet, s'hauran d'establir els processos de coordinació necessaris amb els responsables del diferents serveis que composen el SOC/CERT, amb l'objectiu de garantir l'alineament homogeni amb els diferents objectius establerts.

- **Generació d'informes i indicadors d'estat de l'Orquestració**

El resultat diari dels focus de treball queda documentat mitjançant el desenvolupament de l'informe de "Fets rellevants", el qual es distribueix diàriament a diferents responsables de l'Agència (via correu electrònic). Serà funció del present servei assegurar que l'informe del "Fets rellevants" inclou informació prou rellevant i de valor, així com garantir que es fa arribar a tots els responsables interns que es defineixin, acomplint els temps i canals acordats.

A la vegada, el licitador haurà d'establir els indicadors necessaris per poder monitoritzar l'activitat generada a partir de l'orquestració, i facilitar la presa de decisions.

2.1.2.4 Suport en el seguiment d'objectius estratègics i tàctics

El servei de Governança de l'operativa també és responsable de vetllar per l'assoliment dels objectius estratègics i tàctics de les diferents funcions d'operació de la Ciberseguretat. Per fer-ho, es destaquen les principals tasques a portar a terme:

- Identificar els objectius estratègics i tàctics del SOC/CERT què pugui definir la Direcció del SOC/CERT.
- Garantir el desplegament de la estratègia d'operació de la ciberseguretat de l'Agència.
- Vetllar pel correcte càlcul i alimentació de mètriques i indicadors de l'estat de l'operació de ciberseguretat.
- Vetllar per la correcta disposició de quadres de comandament que permetin la visualització del compliment dels objectius i la presa de decisions de manera senzilla i àgil.
- Fer el seguiment periòdic corresponent del nivell d'objectius assolits per identificar i informar amb prou antelació de possibles desviaments o riscos de no compliment d'aquests objectius.
- Promoure la coordinació de tasques entre els serveis operatius del SOC/CERT per acomplir els objectius definits en els terminis acordats.

2.1.2.5 Coordinació davant esdeveniments puntuals de seguretat

Serà funció d'aquest servei actuar com a reforç de les capacitats de gestió dels equips operatius del SOC/CERT davant situacions puntuals que requereixin d'un seguiment especial o addicional per part de l'àrea d'operacions de seguretat.

A continuació es detallen les accions i funcions principals a desenvolupar per part d'aquest subservei, individualment i de forma transversal, seguint sempre les directrius de la direcció del SOC/CERT.

De forma individual, per a cada un dels processos:

❖ **Operatius de seguretat**

- Obtenció i consolidació de la tota la informació de context dels actius a monitorar durant la duració de l'operatiu, incloent l'estat de situació actual de seguretat en base als àmbits de detecció, prevenció, protecció i resposta.

- Disseny de l'operatiu de ciberseguretat, incloent:
  - Identificació de tots el participants en matèria de ciberseguretat.
  - Definició dels requeriments d'operació de la seguretat de forma coordinada amb la resta de serveis operatius del SOC/CERT i la Direcció de l'Agència.
  - Disseny i definició de model de *reporting.*
- Coordinació del desplegament de l'operatiu, incloent la interlocució amb les parts definides, i el lideratge del seguiment de l'estat de totes les activitats acordades al disseny de l'operatiu.
- Coordinació de l'activació de l'operatiu, assegurant el llançament de les corresponents notificacions, activació dels serveis implicats i acompliment de totes les fites i tasques acordades.

❖ **Seguiments especials de curta durada**

- Obtenció i consolidació de la tota la informació de context dels actius a monitorar durant la duració del seguiment especial, incloent l'estat de situació actual de seguretat en base als àmbits de detecció, prevenció, protecció i resposta.
- Revisió i garantia de la definició d'un model de *reporting*, a mantenir pels equips més operatius implicats en l'execució i seguiment de les tasques durant la duració del seguiment especial.
- Coordinació dels equips operatius del SOC/CERT per assegurar la correcta execució de les tasques definides durant el seguiment especial.

❖ **Gestió de crisis:**

- Lideratge i coordinació dels aspectes administratius i organitzatius envers la funció de l'operació de la ciberseguretat recollits en l'àmbit d'actuació del servei en els diferents comitès de seguiment/crisis endegats per l'Agència.
- Vetllar per la resolució tècnica dels incidents de seguretat crítics i/o d'alt impacte en el negoci, on es compleixin els tres objectius principals: determinar l'afectació/impacte en el negoci, restablir el servei de qualitat el més aviat possible i establir la causa arrel de l'incident.
- Definir i implantar metodologies de gestió de crisis amb l'objectiu de millorar el procés i els procediments actuals que s'utilitzen (poca maduresa, ús mínim d'eines definides, poca agilitat, etc.).
- Registrar i donar visibilitat de forma eficient i amb llenguatge intel·ligible de les accions acordades entre els diferents equips operatius en els comitès de crisis,

mitjançant els canals adients per a cada tipologia i que l'Agència determini (per exemple actes de reunió).

- Definir i implantar metodologies d'anàlisi en la fase post-crisi, de manera coordinada amb l'equip de resposta a incidents que correspongui i la Direcció de l'Agència, amb l'objectiu de millorar els procediments/eines i aconseguir disminuir el nombre de situacions de crisi futures.
- Conèixer i fer ús avançat de les eines implicades en el procés de gestió de crisis, tant les que estiguin vigents en el moment de l'adjudicació del contracte com les que es puguin incorporar durant la vigència del mateix, com a part del servei que presta l'oficina.

De forma transversal:

- Participar en la gestió de casos i esdeveniments importants on l'Agència determini que la presència del servei és necessària, donat l'impacte a negoci que pot tenir una potencial amenaça o incident de seguretat.
- Establir i implantar procediments de revisió i modificació continus (individuals o globals) sobre la informació/documentació/eines que utilitza el servei per garantir que el servei que en proporciona sigui amb qualitat. Per exemple, disposar de la documentació tècnica i funcional d'un servei actualitzada a la darrera versió, determinar modificacions en la informació emmagatzemada als repositoris actuals, etc.
- Proporcionar informes d'incidències sobre els serveis gestionats des de la vessant organitzativa, proposant els canals de comunicació adients per augmentar l'eficiència i l'agilitat extrem a extrem.
- Analitzar, de forma continuada, l'execució dels processos de gestió de crisis amb l'objectiu de detectar, proposar i implantar punts de millora en els propis processos, els procediments relacionats i les eines de gestió emprades, en l'àmbit del propi servei o fora del mateix.

2.1.3 Entrega de valor

Un dels reptes que persegueix el SOC/CERT, com qualsevol altre servei, és la posada en valor la seva funció dintre de la organització. Actualment, l'àrea d'operacions disposa d'una estructura molt important, la qual desenvolupa i genera un conjunt molt significatiu d'iniciatives dintre dels diferents àmbits aplicables (Detecció, Protecció, Prevenció i Resposta). Aquestes iniciatives en tot cas permeten a l'Agència assolir els seus objectius, tant operatius, tàctics i estratègics, sent fonamental disposar d'una capa dedicada per poder presentar adequadament els reptes aconseguits i el benefici que representen. Per tot plegat, serà funció d'aquest lot definir, desenvolupar i generar els conjunt de mètriques, indicadors i lliurables que permetin al SOC/CERT presentar cap a la Direcció les fites assolides.

Per assolir aquest objectiu serà primordial que el servei disposi d'un coneixement clar de com interactuen i quina activitat generen els serveis del SOC/CERT per així aportar una visió integrada i coherent en la construcció i evolució dels indicadors, quadres de comandament i lliurables que generin valor de tota la funció del SOC/CERT.

Les principals tasques que haurà de desenvolupar el present servei són:

- Definició de mètriques i indicadors estratègics, alineats amb els objectius de l'Agència, de cadascun dels serveis que composen el SOC/CERT.
- Explotar el valor de les principals mètriques i indicadors generats pels equips operatius del SOC/CERT de l'Agència, permetent avaluar la consecució dels objectius estratègics de la organització. Aquestes mètriques s'han de poder calcular i consumir mitjançant les eines que es disposen des de l'Agència. Actualment l'eina de presentació d'indicadors utilitzada és Microsoft Power BI.
- Disseny, evolució i millora de quadres de comandament tàctics i estratègics, que permeti disposar per part de la direcció del SOC/CERT d'una visió complerta de l'estat dels indicadors dels diferents serveis.
- Coordinació amb els equips tècnics per la implementació del càlcul d'indicadors i desenvolupament dels quadres de comandament definits.
- Suport en la definició de les diferents plantilles de lliurables per presentar el benefici aportat a l'Agència per part dels serveis del SOC/CERT.
- Establiment d'un procediment de *reporting* periòdic del valor aportat per les diferents línies de servei a la direcció del SOC/CERT.
- Conjuntament amb la direcció del SOC/CERT, s'establiran els períodes d'entrega del *reporting* establert, identificant la periodicitat i el contingut dels mateixos. Aquests lliurables hauran de ser desenvolupats pel present servei.

2.1.4 Volumetries actuals

Per proporcionar una referència per al correcte dimensionament del servei es proporcionen algunes dades de volumetries observades actualment.

Concepte	Quantitat/any
Casos (tiquets) rebuts i gestionats com a primer nivell del SOC/CERT.	**16.700**
Casos escalats a altres serveis del SOC/CERT (via OTRS)	**6.700**
Casos escalats a tercers fora del SOC/CERT (via Remedy)	**4.900**
Trucades rebudes i gestionades	**600**
Revisió de càrrega d'inventaris	**12-15**
Operatius de seguretat	**1**
Esdeveniments especials (però sense categoria d'operatiu)	**3-5**
Gestió de Comitès de crisis	**5-7**
Lliurables d'entrega de valor d'activitats específiques	**5**

Durant l'esdeveniment d'operatius de ciberseguretat s'haurà d'estar preparat per assumir l'activitat necessària per atendre a la prestació del servei segons les necessitats pròpies de l'operatiu, tant de capacitat com d'horari, sense que això suposi, en els primers cinc operatius anuals, un cost addicional per l'Agència.

2.1.5 Lliurables del servei

El licitador ha de tenir en consideració en el model de prestació del servei, la definició, els continguts i la periodicitat dels lliurables del servei i les seves activitats. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència de Ciberseguretat.

Entre els lliurables es poden considerar productes que inclouen fets rellevants diaris de l'activitat operativa dels serveis, seguiment de l'estat de la demanda registrada a tot el SOC/CERT, resums mensuals i anuals 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, notificacions, mètriques i indicadors, entre d'altres.

El llistat que es mostra a continuació, és un mostra dels productes que actualment es lliuren des del servei, indicant la periodicitat definida:

Producte	Periodicitat
Informe de seguiment de l'estat de desplegament de perímetre de sistemes d'informació	Mensual
Informe de seguiment de l'estat de desplegament de perímetre de persones	Mensual
Informe de compliment d'objectius estratègics	Mensual
Informe d'estat de situació del servei	Setmanal
Fets rellevants de l'operativa SOC/CERT	Diari
Memòria anual de l'activitat operativa del SOC/CERT	Anual
Presentació executiva del valor aportat per una o conjunt d'activitats específiques	Puntual
Informe d'estat de la demanda dels principals serveis del SOC/CERT	Setmanal

La relació de productes de la funció de "Governança de l'operació del SOC/CERT", la seva periodicitat i la seva pròpia estructura i continguts s'hauran de definir en la fase inicial abans de la prestació del servei. Aquests 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.

2.1.6 Mètriques i indicadors

Addicionalment als diferents lliurables que pugui generar el servei, aquest també haurà de ser capaç de calcular i facilitar a la capa de "Governança de l'operació del SOC/CERT", funció encarregada de la construcció d'indicadors del SOC, totes aquelles mètriques requerides. Previ a fer la petició, s'haurà de definir i analitzar la seva viabilitat, determinant les fonts necessàries i dades necessàries.

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar pel licitador.

Mètrica	Descripció
Demanda Gestionada	Nombre, tipologia i àmbit de les peticions gestionades pel servei.
Escalat de Peticions	Nombre de tasques realitzades que han estat delegades o escalades a altres serveis, indicant a quin servei concret s'han escalat.
Temps mig d'escalat	Temps mig d'escalat a altres serveis del SOC/CERT, indicant a quin servei concret s'han escalat i tipologia.
Temps mig de resolució	Temps mig de resolució de peticions per servei mensualment.
Peticions sobre actius crítics	Nombre de peticions relacionades amb actius crítics per servei i mes.
Estadístiques de peticions per peticionari	Volumetria i classificació de les peticions rebudes classificada pels principals peticionaris (Departament, àrea interna de l'Agència, etc.) i tipologia de servei sol·licitat.
SICs amb perímetre	Nombre de sistemes d'informació crítics amb cobertura dels serveis que ofereix el model de perímetre de seguretat.
VIPs amb perímetre	Nombre de persones rellevants (alts càrrecs) amb cobertura dels serveis que ofereix el model de perímetre de seguretat.
Vulnerabilitats detectades i comunicades a responsables	Volumetria de vulnerabilitats reportades i corregides a tercers.
Actius amb manca d'informació	Nombre d'actius crítics per als que falta informació per poder desplegar perímetre de seguretat.
Fites assolides	Nombre de fites finalitzades amb èxit en funció de les activitats acordades amb el responsable del servei. S'hauria de poder identificar i comparar el temps de la seva finalització en base a la planificació i abast acordats inicialment.

Mètrica	Descripció
Pla de Capacitat	Càlcul de la capacitat del servei en funció de les tasques realitzades pel servei.
Comitès de crisi gestionats	Nombre de comitès de crisi convocats i liderats per part del Servei, en la funció de coordinació de la crisis.

A més de les llistades per procés, s'hauran de poder obtenir de manera transversal per al servei i l'avaluació dels acords de nivell de servei, com són exemples:

- Nombre de casos/tiquets gestionats pel servei.
- Volum d'hores de dedicació en el servei per cadascun dels membres de l'equip.
- Nombre d'incidències i peticions resoltes segons taula de prioritat en el període.
- Dates d'inici i de lliurament pactat i real de les fites acordades.
- Admissions i desvinculacions de personal de l'equip en el període.

2.2 LOT2: GESTIÓ DE PROJECTES I PLA D'EVOLUCIÓ

El servei d'aquest segon lot és focalitza en la prestació d'un servei de suport a la funció de Gestió de Projectes del servei d'Evolució i transformació del SOC/CERT, que té com a objecte principal la identificació, conceptualització i gestió d'iniciatives (tant tecnològiques com organitzatives) que permetin l'evolució del SOC/CERT, assolint així tots els objectius marcats per l'Agència de Ciberseguretat de Catalunya.

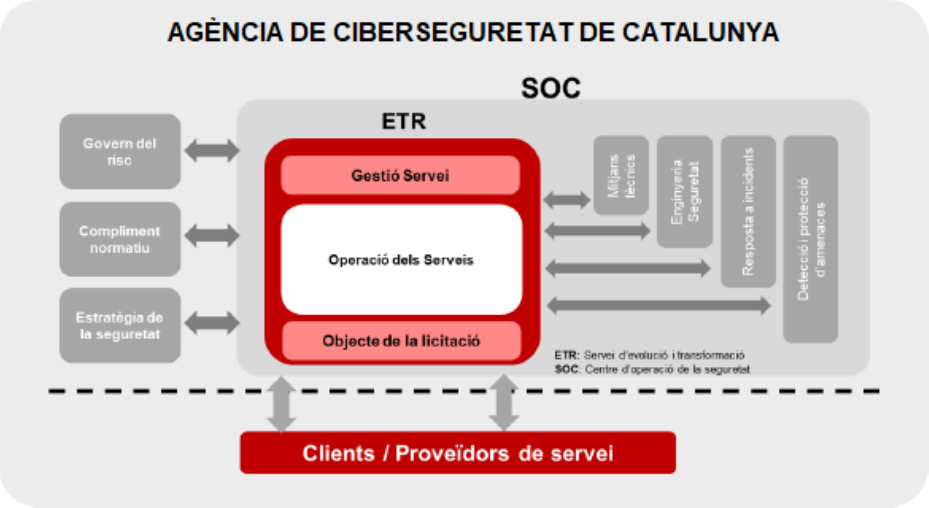

Figura 9. Model de relació actual de la funció ETR a alt nivell

Per tot plegat, el present servei està composat pels següents àmbits de treball:

- Gestió de projectes i iniciatives d'evolució i transformació
- Suport i gestió de necessitats operatives del SOC/CERT
- Desenvolupament del Pla d'Evolució Anual del SOC/CERT

Per tal de regir el disseny del present servei s'ha de tenir en compte els següents principis:

- El servei focalitzarà la seva capacitat en **l'evolució continua dels diferents serveis operatius del SOC/CERT**, coordinant-se amb aquests, i vetllant per l'assoliment conjunt dels objectius estratègics i tàctics de l'Agència.
- Ser responsable de l'elaboració del **Pla d'Evolució Anual del SOC/CERT**
- El servei **avaluarà de forma semestral el nivell de maduresa dels serveis**, i proposarà els plans d'acció i/o transformació necessaris per incrementar-lo.
- El servei **conceptualitzarà i formularà propostes de projecte o iniciatives d'evolució i transformació**, sempre garantint l'alineament d'aquestes amb els objectius estratègics de l'Agència.

- En aquesta línia, **el servei gestionarà els projectes, iniciatives i necessitats del SOC/CERT autònomament**, aportant i/o desenvolupant les metodologies necessàries per gestionar-les el més eficaç possible.
- **El servei circumscriurà i focalitzarà l'estratègia d'evolució a través d'una visió transversal i completa de l'àrea d'operacions**, alhora representant un model de relació àgil i dinàmica.
- **El servei ha de resultar autònom, amb capacitat de lideratge i pressa de decisions**, així com de defensa dels interessos de l'Agència allà on la representi.

Els serveis inclosos en aquest segon lot estan orientat cap a resultats pel que, a final de la seva prestació s'espera haver acomplert els següents objectius:

- **Garantir el desplegament de l'estratègia** del SOC/CERT de l'Agència.
- **Vetllar per l'alineament entre els objectius i l'execució dels serveis** del SOC/CERT.
- Assolir el grau necessari de **lideratge, gestió i control de l'evolució dels serveis** del Centre d'Operació de la Seguretat.
- Donar **compliment a les necessitats de transformació, evolució, correctives i/o estratègiques** que s'originin dins el Centre d'Operació de la Seguretat.
- **Gestionar els projectes tant de caire tecnològic com organitzatiu**, mitjançant una metodologia o estàndard que permeti disposar d'una visió global i particular de l'estat d'aquests, identificant els riscos i millores, així com identificant nous projectes evolutius, si s'escau.
- **Desenvolupament del Pla d'Evolució Anual del SOC/CERT**
- **Incrementar la maduresa del SOC/CERT de l'Agència** perquè aquest resulti més eficaç enfront les ciberamenaces.

Amb l'objectiu de dur a terme satisfactòriament el servei que dona suport a aquestes subfuncions, es desenvoluparan com a mínim les accions que es detallen en els següents apartats.

Els serveis inclosos en aquest segon lot estan orientat cap a resultats pel que, a final de la seva prestació s'espera haver acomplert els següents objectius:

2.2.1 Gestió i suport a projectes i iniciatives d'evolució i transformació

El servei de gestió i suport a projectes i iniciatives d'evolució i transformació del SOC/CERT liderarà, gestionarà i controlarà el seguiment dels projectes, les iniciatives i els plans d'acció i d'evolució del SOC/CERT per tal d'assolir els objectius establerts, assegurant que aquests compleixen amb l'estratègia, requeriments, models i estàndards en l'àmbit de la seguretat de la informació definits per l'Agència.

Alhora, , ja sigui per iniciativa pròpia o a través de les necessitats i els requeriments que els diferents serveis del SOC/CERT de l'Agència expressin, conceptualitzarà i formularà propostes de projecte o iniciatives d'evolució i transformació, on es contemplin de manera detallada la definició dels mateixos, indicant aspectes com el context o situació inicial del negoci envers la necessitat identificada, la justificació de la necessitat detectada / problema a resoldre, la definició del valor o els beneficis esperats pel negoci, o el grau d'alineament de la necessitat amb els objectius estratègics de l'Agència, entre d'altres.

Per tant, és important tenir en compte aquest caràcter dual dels serveis: (i) d'una banda, la prestació de serveis de Ciberseguretat amb la definició de (ii) requeriments i necessitats que configurin la justificació d'iniciatives i projectes, i la seva modelització.

El servei haurà d'aportar el coneixement, la visió i les propostes per orientar les iniciatives en la seva forma i estratègia a partir de la seva experiència en matèria de ciberseguretat i TIC.

2.2.1.1 Suport en la gestió de projectes i iniciatives

El present servei dona suport estructural als responsables dels serveis del SOC, així com als propis serveis, liderant i efectuant el seguiment detallat de les tasques i fites acordades, tant com a projectes o iniciatives (depenent de si són executades de forma interna o no), com les establertes en els diferents plans d'acció i d'evolució dissenyats, amb l'exigència d'assolir els objectius finals establerts garantint els nivells de qualitat marcats per l'Agència de Ciberseguretat de Catalunya.

Addicionalment, s'encarregarà de generar i recopilar els lliurables i la informació rellevant que els projectes i iniciatives generin, traslladant amb visió executiva el valor que emmenen per l'entitat, així com pels diferents àmbits de protecció objecte d'aquesta.

Aquest conjunt d'iniciatives, en funció de la seva complexitat, envergadura i/o inversió associada, poden derivar principalment en dues:

- Iniciatives, les quals tenen una complexitat i unes dependències significatives associades, però que poden ser executades de forma interna amb els recursos

de l'Agència. Com a norma general, aquestes iniciatives no haurien de tenir una duració major a 300 hores de treball.

- Projectes, que requereixen de la seva licitació, i que per la seva complexitat han de ser gestionats de forma acurada, on aspectes com la presa de requeriments, el pas a producció, o la generació de la conseqüent documentació, passen a ser aspectes fonamentals per l'èxit dels mateixos. A la vegada, qualsevol projecte ha de garantir, en tot cas, la flexibilitat i adaptabilitat que un entorn com el SOC/CERT de l'Agència requereix.

El servei establirà un model de relació entre els diferents serveis de l'àrea SOC/CERT, però especialment de forma interna amb el servei d'Arquitectura de Seguretat i Evolució de Solucions, per tal de garantir l'alineació amb els objectius de caire transversal del SOC/CERT.

2.2.1.2 Definició del model en la gestió de projectes i iniciatives

Aquest servei ha d'incorporar la **metodologia de gestió de projectes necessària per a garantir una eficient i efectiva execució dels mateixos, focalitzant-se en el temps i forma d'execució**, complint amb els requeriments, abast i terminis establerts.

Amb aquest objectiu, aquest servei de suport a la gestió de projectes haurà d'establir una línia de treball consistent en:

- **Estandardització de la gestió de projectes**, amb la finalitat d'estalviar temps i millorar la qualitat del treball. Així, a través d'aquesta estandardització, es pretén disposar d'un enfocament metodològic, d'un control dels processos a executar dins el cicle de vida dels projectes de ciberseguretat, de la procedimentació a seguir per dur a terme les operacions repetitives, i de plantilles a utilitzar de cara a la generació dels lliurables.

- **Seguiment global de l'estat dels projectes**, gràcies a la estandardització prèviament definida, caldrà dur a terme un seguiment general basat en l'aplicació de metodologies, recopilació i seguiment dels indicadors i mètriques per a la cartera de projectes. Aquestes seguiment ha de ser consumible de manera àgil i centralitzada, permetent la identificació del resultat de l'exercici dels projectes, tendències, desviacions de temps, discrepàncies i èxits en base els requeriments i fites definides.

- **Aplicació de bones pràctiques en el camp de la gestió de projectes**, dirigida a prioritzar la cartera de projectes i la presa de decisions crítiques, entre d'altres.

- **Industrialització del procediment de gestió de projectes**, amb l'objectiu d'evitar la pèrdua de coneixement generada principalment a causa de la rotació de personal.

A través de la metodologia sol·licitada es pretén que el servei prioritzi i alineï estratègicament les iniciatives i projectes, això com que susciti la generació d'informes d'acord amb el valor i beneficis reportats. Es requerirà, per tant, la participació del servei de suport en la gestió de projectes en la planificació estratègica i l'assessorament als responsables dels serveis del SOC/CERT, així com als propis serveis, en la presa de decisions.

Un cop realitzada la conceptualització de projectes i iniciatives d'evolució, hauran de ser validades i aprovades per la direcció del SOC/CERT, sent fonamentant poder defensar la necessitat de la execució de la iniciativa o projecte en funció d'aspectes com el seu grau d'alineament amb els objectius de l'Agència, el valor aportat per la iniciativa o el projecte, o el retorn de la mateixa. Per tot plegat, serà fonamental que l'adjudicatari disposi del coneixement necessari per poder executar aquesta fase fonamental de forma efectiva.

El servei haurà de liderar (juntament l'equip de projecte definit -recursos interns del SOC/CERT i/o externs-), les tasques pròpiament de planificació, com són la definició dels requeriments detallats, identificats pel personal especialitzat de l'equip de treball, l'estimació de temps i costos, o la definició de la planificació del projecte (recursos, pressupost, fases, fites, tasques, etc.). Com a resultat d'aquesta fase, l'adjudicatari haurà de generar (o responsabilitzar-se de que es generi) un document on es reculli tota la informació del projecte o iniciativa: "pla de projecte", així com en fase de tancament, de la tramitació de la documentació, informes i lliurables finals adreçats a la direcció del SOC/CERT.

Finalment, el licitador haurà de tenir en consideració la necessitat d'implantar els processos transversals necessaris per la gestió de manera eficient de les diferents iniciatives d'evolució o projectes que puguin ser necessaris. En aquest sentit, alguns dels principals processos a tenir en consideració són:

- **Gestió de la capacitat** en quant a activitats com: actuacions, projectes i altres accions que es sol·licitin. S'espera del servei pugui indicar, mitjançant KGI's/KPI's de servei, la seva capacitat d'execució de les activitats esmentades, adquirint un compromís amb les parts interessades.
- **Gestió de la comunicació.** En tot moment, totes les parts interessades han de poder tenir coneixement de l'estat del projecte en quant aspectes crítics com són les fites assolides, el valor aportat, o les desviacions (en temps, costos o recursos).
- **Gestió del canvi.** Tot canvi dintre del projecte que sigui significatiu, haurà de ser registrat i inclòs en les mètriques del servei per a poder mesurar i treure conclusions sobre l'eficàcia i eficiència de la metodologia emprada en el propi projecte, a fi i efecte de poder evolucionar la mateixa.

- **Gestió del risc.** És funció del present servei, la detecció de riscos que puguin afectar per una banda al propi projecte, posant en perill l'assoliment dels beneficis esperats amb el grau de qualitat i planificació acordada amb el promotor, i per l'altre, els riscos de seguretat que el propi projecte pugui detectar en qualsevol de las fases que el conformen (cas de negoci, conceptualització, planificació, execució, entrega i tancament).

2.2.2 Suport i gestió de les necessitats operatives del SOC/CERT

El servei de gestió i suport a les necessitats operatives del SOC/CERT afrontarà les necessitats d'evolució i transformació detectades dins l'àrea d'operacions de la seguretat, que no es poden tractar dins l'àmbit dels serveis recurrents del SOC/CERT.

Les principals tasques a desenvolupar en l'àmbit d'aquesta funció seran:

- Donar suport a la gestió de necessitats operatives d'evolució als diferents serveis del SOC/CERT, proveint d'expertesa i coneixement de seguretat a la tasca de definició i concreció d'aquestes iniciatives que s'endeguin dins de la pròpia àrea, sempre d'acord amb la metodologia de gestió de projectes, iniciatives i necessitats, definit pel licitador.
- Aquestes tasques operatives, que es gestionen des de la ETR, requereixen en molts casos la comunicació amb tercers (proveïdors, CTTI...) per poder ser executades.
- Dotar del criteri tècnic necessari per valorar la viabilitat d'aquesta necessitat operativa, en termes de qualitat, seguretat, costos, esforç i sobre tot, valor i beneficis per l'organització i els seus clients.
- Supervisió i seguiment del progrés de resolució de les necessitats operatives, amb l'objectiu de disposar dels mecanismes necessaris per valorar l'avenç de resolució de la necessitat i facilitar la presa de decisions, si s'escau.

2.2.3 Pla d'Evolució del SOC/CERT

El servei d'Evolució i Transformació te com a funció principal la millora de les capacitats del SOC/CERT de l'Agència, perquè aquest resulti més eficaç enfront les ciberamenaces. Augmentant progressivament les seves capacitats es pretén dotar al SOC/CERT en:

- Prevenció davant de les vulnerabilitats que els sistemes d'informació i suports que sustenten els processos dels diferents àmbits d'actuació de l'Agència de Ciberseguretat.

- Protecció, tants dels sistemes d'informació com dels usuaris dels mateixos (i la seva informació), davant dels ciberatacs que fan focus sobre els àmbits de l'Agència.
- Detecció de noves ciberamenaces que puguin afectar la operació normal dels processos de negoci competència de l'Agència.
- Resposta davant d'incidents de ciberseguretat que suposin pèrdues tant econòmiques, com organitzatives o d'imatge.

Per tant, entre d'altres, podem dir que la funció principal i en termes generals d'aquest servei és la Gestió de l'Evolució del SOC, procés el qual inclou, entre d'altres, les següents tasques:

- **Elaboració del Pla d'Evolució Anual del SOC/CERT** amb la finalitat d'identificar i assolir els objectius d'evolució del mateix, garantint-ne l'alineament amb els objectius estratègics de l'Agència, i **vetllant per l'assoliment dels mateixos**.
- **Definició dels plans d'acció i/o transformació**, a fi i efecte de desplegar el Pla d'Evolució i d'augmentar el nivell de maduresa del serveis del SOC/CERT, liderant la seva implementació conjuntament amb els responsables dels serveis corresponents.
- **Càlcul semestral del nivell de maduresa dels serveis del SOC/CERT** mitjançant la utilització de la metodologia d'aquest, basada en els models del SOC-CMM i la NIST.
- **Evolució del mètode de mesura de la maduresa dels serveis del SOC** (incloent l'ETR), el qual dona resposta als àmbits principals sobre els que versen les activitats del SOC/CERT de l'Agència.

Aquest servei haurà de disposar d'un model de relació entre els diferents serveis de l'àrea SOC/CERT, però especialment de forma interna amb el servei d'Arquitectura de Seguretat i Evolució de Solucions, per tal de garantir l'alineació amb els objectius de caire transversal del SOC/CERT.

Aquest servei serà responsable de donar resposta, entre d'altres, a les següents funcions:

2.2.3.1 Elaboració del Pla d'Evolució Anual del SOC/CERT

Dins de la prestació del servei, **s'haurà de plantejar un Pla d'Evolució Anual del SOC/CERT** amb la finalitat d'assolir els objectius d'evolució del mateix, amb l'eficiència necessària en el model de relació i la coordinació amb la resta de serveis de l'ETR, i constituint un punt central per la canalització de peticions del Centre d'Operació de la Seguretat (iniciatives, necessitats, projectes, etc.).

Aquest Pla d'Evolució Anual caldrà que sigui presentat pel servei durant el quart trimestre de l'any anterior al de la seva execució. Així mateix, aquest servei serà responsable del Pla d'Evolució Anual vigent en el primer any d'execució del contracte.

2.2.3.2 Definició dels plans d'acció i/o transformació

El present servei és el **responsable de la gestió dels plans de transformació endegats o presentats**, pels diferents serveis del Centre d'Operació de la Seguretat. L'objectiu d'aquesta gestió és garantir que les diferents fites descrites en els plans de transformació s'assoleixen en els terminis definits i amb la qualitat òptima per tal d'aportar un valor i una millora continua dels propis serveis. Es responsabilitat del servei la realització d'aquesta tasca, per la qual **definirà i implementarà la metodologia que consideri adient**.

Es també objecte d'aquest servei la gestió de les diferents actuacions fruit dels plans d'acció corresponents, entenent per actuació, aquelles activitats que no arriben a tenir entitat de projecte pel nivell de complexitat, esforç i costos associats i que es tradueixen sovint en tasques o accions a curt-mig termini amb dedicació a temps parcial d'un únic recurs. No obstant, donada la importància que algunes d'aquestes actuacions representen per la consecució d'objectius de més alt nivell, cal realitzar una planificació i seguiment acurat amb les diferents parts implicades.

Els plans de transformació i les actuacions poden tenir com a sol·licitant algun dels serveis del SOC/CERT o bé el propi servei qui, en el continu exercici d'anàlisi de l'efectivitat, qualitat i eficiència dels serveis del SOC/CERT, detecti una oportunitat de generació de valor per l'entitat o necessitat a curt termini per corregir una situació contraproduent o de risc.

En tot cas, **els diferents plans de transformació hauran de garantir l'alineament amb els objectius estratègics de l'Agència**, vetllant per l'assoliment dels mateixos. Per aquest fet, serà funció a la vegada del present servei la identificació de la capacitat necessària per l'execució dels plans.

Un cop analitzats els diferents plans de transformació, el servei prioritzarà i calendaritzarà les tasques juntament amb els proveïdors, d'acord amb els objectius d'evolució i transformació de l'àrea del SOC/CERT, amb l'objectiu principal de liderar les millores dels serveis amb un total alineament amb els objectius estratègics de l'Agència.

2.2.3.3 Càlcul del nivell de maduresa dels serveis del SOC/CERT

El licitador presentarà, desenvoluparà i desplegarà una metodologia de gestió de la maduresa basada en els estàndards de referencia del NIST FRAMEWORK i el SOC-CMM, i adaptada a les especificacions dels serveis del SOC/CERT de l'Agència. Aquesta metodologia, un cop presentada, serà validada per la direcció del SOC/CERT prèviament al seu desenvolupament i desplegament.

Seguidament, **serà responsabilitat del present servei el càlcul semestral de la maduresa dels serveis del SOC/CERT**, establint els informes necessaris per presentar les conclusions i resultats obtinguts a tots els nivells:

- **Operatius**, incloent tant els equips de treball existents, com els responsables dels serveis del SOC/CERT.
- **Tàctics**, presentant les principals conclusions del nivell de maduresa als responsables dels serveis i responsables de línia de servei.
- **Estratègics**, sent els receptor dels mateixos la Direcció del Centre d'Operació de la Seguretat.

2.2.3.4 Evolució del mètode de mesura de la maduresa

El SOC/CERT és un àrea en evolució constants en totes les seves vessants, tant tècniques, per mitjà de la evolució constant de les solucions que sustenten els principals processos de l'àrea, com organitzatives, a través de la inclusió o modificació de les funcions i rols establerts a l'àrea.

Derivat d'aquest fet, és fonamental que la metodologia de gestió de la maduresa existent s'adapti a la pròpia evolució del SOC, sent tasca fonamental del present servei. D'aquesta forma, l'adjudicatari haurà d'establir un procés de revisió i evolució continua de la metodologia de gestió de la maduresa.

2.2.4 Volumetries actuals

Per proporcionar una referència per al correcte dimensionament del servei es proporcionen algunes dades de volumetries observades actualment.

Concepte	Quantitat/any
Gestió de Projectes i Pla d'Evolució	
Projectes gestionats	**60**
Iniciatives CTTI gestionades	**35**
Necessitats del SOC/CERT gestionades	**70**
Pla d'Evolució del SOC/CERT	**1**
Informes de maduresa	**2**
Plans d'acció	**5**

2.2.5 Lliurables del servei

El licitador ha de tenir en consideració en el model de prestació del servei, la definició, els continguts i la periodicitat dels lliurables del servei i les seves activitats. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència de Ciberseguretat.

Entre els lliurables es poden considerar productes que inclouen el seguiment de l'estat de situació dels projectes, les necessitats o les iniciatives, presentacions de caire estratègic o tàctic vers l'estat de situació del pla d'evolució del SOC/CERT, presentacions adreçades a la direcció del SOC/CERT o la Direcció General de l'ACC vers l'estat del servei en qüestió, resums mensuals i anuals de l'activitat del servei, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, mètriques i indicadors, entre d'altres.

El llistat que es mostra a continuació, és un mostra dels productes actualment es lliuren des del servei, indicant la periodicitat definida:

Producte	Periodicitat
Informe i quadre d'estat de servei	Mensual
Informe i quadre de seguiment dels projectes, necessitats i iniciatives	Setmanal
Informe executiu de l'estat d'evolució dels projectes	Quinzenal
Informe de l'estat de la maduresa	Semestral
Pla d'Evolució del SOC/CERT	Anual
Informe executiu de l'estat d'evolució anual del SOC/CERT	Semestral

La relació de productes de la funció de "Gestió de Projectes i Pla d'Evolució", la seva periodicitat i la seva pròpia estructura i continguts s'hauran de definir en la fase inicial abans de la prestació del servei. Aquests 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.

2.2.6 Mètriques i indicadors

Addicionalment als diferents lliurables que pugui generar el servei, aquest també haurà de ser capaç de calcular i facilitar a la capa de "Evolució i Transformació", funció encarregada de resoldre necessitats del SOC/CERT, evolucionant-lo cap a una gestió eficaç i eficient de les ciberamenaces, totes aquelles mètriques requerides.

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar pel licitador.

Mètrica	Descripció
Projectes, necessitats i iniciatives gestionades	Nom, número i estat dels projectes, necessitats i iniciatives gestionades pel servei.
Projectes assolits en termini	Nombre i percentatge de projectes assolits d'acord als terminis de finalització definits.
Projectes amb retard acumulat	Nombre i percentatge de projectes oberts o pendents que no compleixin els terminis de finalització definits, incloent tipologia o motivació de l'endarreriment.
Projectes finalitzats satisfactòriament	Nombre i percentatge de projectes finalitzats amb assoliment satisfactori dels objectius i fites.
Temps mig de tancament de projecte / iniciativa / necessitat	Temps mig de tancament dels projectes / iniciatives / necessitats, segregats per tipologia.
Temps mig de retard per projecte / iniciativa / necessitat	Temps mig de retard dels projectes / iniciatives / necessitats, segregats per tipologia.
Capacitat per projecte / iniciativa / necessitat	Capacitat mitja requerida per la gestió efectiva dels projecta / iniciativa / necessitat
Grau d'assoliment del Pla d'Evolució Anual	Grau d'assoliment i completessa del Pla d'Evolució del SOC/CERT
Grau d'assoliment del Pla d'Acció	Grau d'assoliment i completessa dels diferents Plans d'Acció elaborats pel servei

A més de les llistades per procés, s'hauran de poder obtenir de manera transversal per al servei i l'avaluació dels acords de nivell de servei, com són exemples:

- Volum d'hores de dedicació en el servei per cadascun dels membres de l'equip.
- Dates d'inici, fites i objectius acordats en les iniciatives, necessitats i projectes.
- Admissions i desvinculacions de personal de l'equip en el període.

2.3 LOT 3: ARQUITECTURA DE SEGURETAT I EVOLUCIÓ DE SOLUCIONS

El servei objecte de la present licitació es focalitza en la prestació d'un servei de suport a la funció d'Arquitectura i Evolució de les solucions de ciberseguretat del SOC/CERT, que té com a objectius principals l'avaluació i disseny de la seguretat dels entorns tecnològics competència de l'Agència, millorar l'eficiència i l'eficàcia dels serveis del SOC/CERT a través de la industrialització i l'automatització dels seus processos i l'evolució de les solucions de Ciberseguretat, donant compliment a les necessitats de transformació i evolució que s'originen dins el SOC/CERT.

Per tot plegat, el present servei es compon dels següents àmbits de treball:

- Arquitectura de seguretat dels ens públics.
- Evolució de solucions de Ciberseguretat.

A continuació es llisten les principals funcions que regeixen el disseny del present servei de suport i la seva licitació:

- **Disseny, identificació i validació d'arquitectures i solucions tecnològiques de seguretat** que afectin l'àrea d'operacions de la seguretat en projectes de nova implantació i/o transformació de l'entorn TIC de la Generalitat de Catalunya i dels seus àmbits.
- **Definició dels models de govern operatiu de la seguretat** del SOC/CERT per les entitats públiques.
- Suport expert en la **identificació de noves solucions de Ciberseguretat** que evolucionin les diferents funcions del SOC/CERT.
- **Evolució de les principals solucions transversals del SOC/CERT**, per tal de millorar l'eficiència de les tasques desenvolupades per l'àrea i potenciar l'entrega de valor al negoci.
- **Rendibilització dels processos** dels serveis del SOC/CERT **mitjançant l'automatització i optimització** dels mateixos.
- **Suport expert tecnològic a la resta de serveis del SOC/CERT**, especialment al Lot2 d'aquesta licitació, en la definició de requeriments d'arquitectura de seguretat, integració entre solucions de seguretat, registre d'informació als repositoris del SOC/CERT, entre d'altres

A més, i tenint en compte l'orientació cap a resultats del servei, al final de la prestació del mateix s'hauria d'acomplir els objectius que es llisten a continuació:

- Definir l'arquitectura de seguretat dels ens públics.
- Establir els models de govern operatiu de la seguretat de les entitats públiques.
- Identificar noves solucions tecnològiques pel SOC/CERT
- Millorar l'eficiència i l'eficàcia dels serveis del SOC/CERT a través de la industrialització i automatització dels seus processos.
- Desenvolupar i evolucionar les solucions tecnològiques transversals del SOC.

Amb l'objectiu de dur a terme satisfactòriament el servei que dona suport a aquestes subfuncions, es desenvoluparan com a mínim les accions que es detallen en els següents apartats.

2.3.1 Arquitectura de seguretat dels ens públics

El servei d'Arquitectura de Seguretat té com a principal objectiu el d'assegurar que els projectes i iniciatives TIC del SOC/CERT del compleixen amb els requeriments, models i estàndards en l'àmbit de la seguretat de la informació.

També és funció d'aquest servei donar suport a l'Agència de Ciberseguretat en quan a la validació i definició d'arquitectures de seguretat en projectes de nova implantació, així com transformacions de l'entorn TIC sota l'abast de la pròpia Agència.

Alhora, el servei d'Arquitectura de Seguretat té com a funció la identificació i proposta de noves solucions tecnològiques que puguin ser d'aplicabilitat a la operació de la seguretat del SOC/CERT.

El servei d'Arquitectura de Seguretat, serà responsable de donar resposta, entre d'altres, a les següents funcions:

2.3.1.1 Disseny i creació de models d'arquitectura de seguretat

Les principals tasques a desenvolupar en l'àmbit d'aquesta funció seran:

- Disseny d'arquitectures de seguretat per a la implantació de nous serveis dintre del SOC/CERT, projectes o solucions. Això inclou, entre d'altres:
  - Diagrames de topologia lògica o topologia física
  - Representació dels fluxos de tràfic, explicant el detall de cadascun d'ells (Internet, Intranet, xarxa interna, xarxa de producció, xarxa d'administració, etc.)

- Inventari d'equipaments i adreçaments (VLAN's, protocols d'enrutament, IPs, @MAC, etc.)

- Creació i suport en la creació d'arquitectures de seguretat per l'evolució i transformació de serveis existents del SOC/CERT.
- Garantir que aquests models d'arquitectures de seguretat són integrables amb els elements de seguretat que conformen el perímetre de seguretat del SOC/CERT.
- Creació de models d'arquitectura de seguretat homogenis i industrialitzables pels diferents àmbits que composen el SOC/CERT, definint i establint aquests models de govern operatiu de la seguretat del SOC/CERT per les entitats públiques.
- Garantir que tots aquests models i dissenys són operables i/o governables per part del SOC/CERT i que son específics, mesurables, assolibles, rellevants i panificables (model SMART).

2.3.1.2 Validació d'arquitectures i solucions de TI / seguretat

Les principals tasques a desenvolupar en l'àmbit d'aquesta funció seran:

- Validar les arquitectures i funcionalitats de seguretat de les solucions TIC que afecten a l'entorn d'operació del SOC/CERT de l'Agència o poden afectar en un futur.
- Donar suport a l'assegurament que els serveis, sistemes d'informació i usuaris objecte de control per part del SOC/CERT, estan sota els perímetres de seguretat del propi SOC/CERT, tant tecnològicament com organitzativament.
- Validar que la informació existent sobre les arquitectures dels serveis i les solucions és la necessària per poder valorar la seguretat de la implantació i del seu entorn

2.3.1.3 Identificació de noves solucions de seguretat pel SOC/CERT

Serà part de la funció d'aquest servei, a través dels corresponents exercicis de consultoria tecnològica, **la identificació i proposta de noves solucions tecnològiques** que poguessin ser d'aplicabilitat a la operació de la seguretat i que es puguin desplegar amb l'objectiu de potenciar, evolucionar i enfortir les capacitats de protecció, prevenció, detecció i resposta de l'Àrea d'Operacions.

2.3.2 Evolució de solucions de Ciberseguretat del SOC/CERT

La principal tasca a desenvolupar en l'àmbit d'aquesta funció serà el desenvolupament del diferent programari que sustenta els principals processos implementats al SOC/CERT de l'Agència per mitjà de la industrialització dels mateixos, i la identificació de noves solucions de seguretat així com l'evolució de les principals solucions transversals de seguretat de l'Àrea d'Operacions, per tal de millorar les capacitats desplegades des de l'àrea.

2.3.2.1 Suport al desenvolupament de programari

El present servei té com a objectius principals:

- La millora dels processos del SOC mitjançant la automatització i optimització dels mateixos.
- El desenvolupament de solucions especifiques pel SOC que permetin millorar la eficiència de les tasques desenvolupades per l'àrea i potenciar l'entrega de valor al negoci.
- La gestió de la demanda generada pels diferents serveis relacionada amb el desenvolupament d'evolutius del vigent programari.

Concretament, i pel que fa als conceptes d'automatització i d'industrialització, l'àrea de suport a la evolució de solucions de ciberseguretat tindrà com a tasques principals:

- El desenvolupament del programari necessari (principalment mitjançant scripts) per poder millorar la industrialització dels processos dels SOC/CERT a través de la millora.
- L'evolució continua de la solució INFOSOC del SOC/CERT, eina específica creada per l'Agència de Ciberseguretat de Catalunya, que té com a objectiu principal la generació dels indicadors, tant operatius, tàctics i estratègics, del SOC/CERT. Aquesta solució té actualment integrats més de 15 solucions de l'àrea d'operacions de seguretat, analitzant en temps real la seva activitat. A partir de la mateixa, i de la intel·ligència que té implementada, genera de forma automàtica o, en alguns casos, a través de càrregues manuals, els indicadors definits per cada Línia de Servei del SOC/CERT. A nivell informatiu, aquesta solució es troba desenvolupada principalment en *Django / Phyton*.

  Altrament, l'evolució de la solució Power BI també s'identifica com a tasca cabdal del servei, ja que aquesta té la funció d'analitzar fonts de dades i presentar-les en forma de quadres de comandament requerits pels diferents serveis del SOC/CERT.

És aspecte fonamental del present servei la gestió eficient de la demanda generada pels diferents serveis del SOC/CERT de l'Agència, sent necessari establir processos eficients per la seva valoració, priorització i gestió del *backlog* existent. Per aquest fet, l'Agència ha implementat procediments basats en metodologia *Agile*.

2.3.2.2 Evolució de solucions de Ciberseguretat

La principal tasques a desenvolupar en l'àmbit d'aquesta funció és l'evolució de les solucions transversals i crítiques de seguretat que opera el SOC/CERT, amb l'objectiu de millorar les capacitats de detecció, prevenció, protecció i resposta de l'Àrea d'Operacions a través del desplegament de noves funcionalitats, optimitzar-ne el rendiment operatiu, millorant el retorn de la inversió automatitzant tasques operatives, entre d'altres.

Dins el ventall de solucions que regularment usa el SOC/CERT, s'identifiquen de manera inequívoca i a mode d'exemple les següents, no sent aquesta relació excloent podent-se identificar d'altres que puguin resultar d'interès:

- Organització, automatització i resposta de la seguretat (SOAR), en referència a la solució encarregada de la gestió de casos i fluxos de treball, automatització de les tasques, i centralització per accedir a la informació sobre les amenaces, fer consultes i compartir dades.
- Gestió de la informació i els esdeveniments de seguretat (SIEM), com a solució de monitoratge i anàlisi d'esdeveniments en temps real, així com també de seguiment i registre de dades de seguretat.
- Repositori centralitzat de seguretat (Data Lake), com a solució destinada a mantenir i gestionar tots els registres o fonts de dades rellevants per a la postura de seguretat del SOC/CERT.

2.3.3 Volumetries actuals

Per proporcionar una referència per al correcte dimensionament del servei es proporcionen algunes dades de volumetries observades actualment.

Concepte	Quantitat/any
Arquitectura	
Definicions de models de perímetre de seguretat	**3**
Documents de models operatius	**5**
Casos d'ús dissenyats per implementar a les principals solucions de ciberseguretat	**30**
Validació de documents de disseny d'alt nivell, de projectes i iniciatives	**15**

Concepte	Quantitat/any
Projectes on s'ha prestat suport expert en matèria d'arquitectura de seguretat	**20**
Dissenys de models d'aproximació de serveis de SOC sobre nous entorns	**2**
Evolució de solucions	
Tasques d'automatització de processos	**30**
Desenvolupament de noves funcionalitats a repositori central d'informació del SOC/CERT	**40**
Correcció de '*bugs'* al repositori central d'informació del SOC/CERT	**10**
Desenvolupament de quadres de comandaments (PowerBI)	**15**

2.3.4 Lliurables del servei

El licitador ha de tenir en consideració en el model de prestació del servei, la definició, els continguts i la periodicitat dels lliurables del servei i les seves activitats. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència de Ciberseguretat.

Entre els lliurables es poden considerar models de perímetre de seguretat, models d'operació de la seguretat, presentacions de caire estratègic o tàctic vers l'estat de situació del servei adreçades a la direcció del SOC/CERT o la Direcció General de l'ACC, informes de caire evolutiu de caire tecnològic o organitzatiu, resums mensuals i anuals de l'activitat del servei, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, mètriques i indicadors, entre d'altres.

El llistat que es mostra a continuació, és un mostra dels productes actualment es lliuren des del servei, indicant la periodicitat definida:

Producte	Periodicitat
Informe i quadre d'estat del servei	Mensual
Informe i quadre de seguiment dels models, dissenys, necessitats, automatitzacions.	Setmanal
Informe executiu de l'estat dels models, dissenys, necessitats, automatitzacions.	Quinzenal
Informe executiu de la evolució i les millores aconseguides per part del servei.	Semestral
Informe de model, disseny, necessitat o automatització implementada per part del servei.	Puntual
Informe de *benchmark* realitzat per part del servei.	Puntual.

La relació de productes de la funció, la seva periodicitat i la seva pròpia estructura i continguts s'hauran de definir en la fase inicial abans de la prestació del servei.

Aquests 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.

2.3.5 Mètriques i indicadors

Addicionalment als diferents lliurables que pugui generar el servei, aquest també haurà de ser capaç de calcular i facilitar al seu responsable i capes de presa de decisions, una sèrie de mètriques i indicadors relacionats.

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar pel licitador.

Mètrica	Descripció
Models d'arquitectura de seguretat dissenyats	Número de models d'arquitectura de seguretat dissenyats.
Documents de disseny validats	Número de documents de disseny d'arquitectures validats.
Fluxos de tràfic inventariats	Número de fluxos de tràfic inventariats per part del servei i posats a disposició per el conjunt de serveis del SOC.
Models operatius elaborats	Número de models operatius on el servei ha participat i ha sigut part activa per a la definició i publicació del model.
Casos d'ús dissenyats	Número de casos d'ús que els servei ha dissenyat/millorat i que estan en ús per part del serveis del SOC.
Projectes on s'ha prestat suport	Número de projectes on el servei ha participat de forma activa durant les diferents fases de les que consten els projectes.
Industrialització de processos	Número de processos operatius del SOC que s'han automatitzat exitosament.
Guany d'eficiència per automatització	Valoració del guany (econòmic, temporal, etc.) d'eficiència assolit amb la automatització implementada del procés operatiu del SOC.
Playbooks implementats	Número de *playbooks* implementats a la eina SOAR.
Suport tècnic expert a la resolució d'incidències de les solucions del SOC/CERT	Número d'incidències ateses en relació a incidències detectades a les solucions del SOC/CERT.

Mètrica	Descripció
Noves funcionalitats al repositori central	Número de funcionalitats noves o errors corregits que s'han implementat a les eines transversals del SOC.
Quadres de comandament	Número de quadres de comandament implementats a les eines de visualització analítica del SOC.
Grau de capacitat del servei	Capacitat mitja requerida per la gestió efectiva de les necessitats/models/dissenys del servei.

A més de les llistades per procés, s'hauran de poder obtenir de manera transversal per al servei i l'avaluació dels acords de nivell de servei, com són exemples:

- Nombre de tiquets en el servei.
- Volum d'hores de dedicació en el servei per cadascun dels membres de l'equip.
- Nombre d'incidències i peticions resoltes segons taula de prioritat en el període.
- Dates d'inici i de lliurament pactat i real de fites.
- Admissions i desvinculacions de personal de l'equip en el període.
- Puntuacions de satisfacció de lliurables.

3 CONDICIONS D'EXECUCIÓ

Aquest capítol descriu els requisits d'execució dels serveis que s'han de tenir en compte a l'hora d'elaborar les propostes, a més dels addicionalment inclosos a la resta del present document.

3.1 Consideracions generals

- El licitador haurà de ser capaç d'executar els mecanismes adients per tal de fer la integració operativa amb els processos del CTTI (p. ex. obtenció d'informació, consultes a l'inventari d'actius, llançament de peticions i RFC necessàries per a desplegar les mesures de seguretat, aplicació de contramesures, integració amb el Centre de Control, CTTI, identificació d'interlocutors necessaris en els àmbits, integració amb l'equip SAU CTTI...), així com canalitzar les comunicacions necessàries per a les vies i eines establertes.

- El licitador ha de tenir en compte els criteris d'industrialització a l'hora de definir i pensar en els serveis, processos, procediments i eines, i per tant, evitar propostes de serveis que exigeixin: (i) Processos que consumeixin grans esforços de recursos; (ii) Eines amb baix retorn, tant d'eficiència com d'eficàcia; (iii) Processos monolítics i aïllats, que no puguin revertir en millores d'altres processos i serveis, i; (iv) Coneixements tancats, que no comuniquin i que impedeixen el creixement de l'organització. L'anterior ha d'estar **degudament documentat**, demostrant la línia d'industrialització plantejada i tenint en compte quins processos i eines poden ser requerides.

- El licitador ha de determinar l'existència de lliurables, el seu contingut i la seva periodicitat que consideri donen resposta o poden millorar la prestació o percepció del servei per part de l'Agència.

- El licitador pot millorar i completar les mètriques i productes i lliurables senyalats per l'Agència en els respectius lots.

3.2 Horaris

Els serveis s'hauran de prestar d'acord amb els horaris especificats a continuació:

BLOC DE SERVEI	HORARI DE PRESTACIÓ
Lot 1: Governança de l'operativa del SOC/CERT	• Gestió de la Demanda: 12x5 en horari de dies laborables, amb guàrdia per al suport en comitès de crisi. • Resta de serveis: 8x5 • Gestió de Comitès de Crisis: 24x7 en format guàrdia.
Lot 2: Gestió de projectes i Pla d'Evolució **Lot 3: Arquitectura de seguretat i Evolució de solucions**	• 8x5

Es considera horari de dies laborables els dies que siguin laborables a qualsevol dels centres de treball dels clients que fan ús dels serveis amb prestació ininterrompuda de 8:00h a 20:00h.

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.

Es requereix que la prestació del servei objecte de licitació sigui continua durant els 12 mesos de l'any, es a dir, la capacitat requerida ha de ser la mateixa, havent de cobrir el licitador els períodes de vacances amb els recursos necessaris.

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, amb acord previ entre l'Agència i l'adjudicatari.

A petició de l'Agència, els adjudicataris resultants d'aquest plec hauran de donar suport presencial als diferents clients. Els adjudicataris han de contemplar que, ocasionalment, aquest suport es pot produir fora de l'horari laboral habitual de l'Agència.

Si durant l'execució del contracte l'Agència o els adjudicataris detecten la necessitat de modificar l'horari de servei d'algun dels serveis o equips descrits en aquest plec, l'Agència i els adjudicataris consensuaran de forma conjunta la modificació, essent l'Agència qui finalment designi l'horari de prestació que s'adeqüi a les necessitats pròpies i dels clients i que no perjudiqui de forma excessiva a l'adjudicatari.

3.3 Localització Física

Els equips prestataris dels serveis poden operar remotament i a les pròpies dependències de l'Agència, si així ho requereix aquesta. La ubicació presencial a les oficines de l'Agència de Ciberseguretat ubicades a l'Hospitalet de Llobregat serà puntual i vindrà determinada pel Responsable de Línia de Servei corresponent. Addicionalment, fora dels dies acordats amb el RLS la presencialitat podrà donar-se quan el servei ho consideri necessari, per poder aprofitar les capacitats de les instal·lacions de l'Agència de Ciberseguretat, però sempre i quan aquest fet sigui requerit per la prestació del servei i el RLS ho hagi autoritzat prèviament.

Les instal·lacions, edificis i dependències utilitzats per a la prestació d'aquest servei hauran de complir en qualsevol moment amb tots els requisits de construcció, habitabilitat, seguretat i ergonomia estipulats per la normativa de règim local del municipi a on es trobi, de la Generalitat de Catalunya i de l'Estat en la seva expressió més exigent.

Es tindrà en consideració el poder disposar de presencialitat física a les instal·lacions de l'Agència, dins d'un termini de temps raonable donada una situació d'excepcionalitat.

Finalment, els licitadors també hauran d'incloure en la seva oferta la provisió d'instal·lacions de contingència.

3.4 Estructura dels serveis licitats

3.4.1 Recurrent o servei base

El licitador haurà d'aportar una definició de serveis recurrents per a donar cobertura al servei licitat, corresponent a l'àrea del SOC/CERT. Aquest servei recurrent ha de permetre cobrir l'operativa ordinària de l'Agència i donar capacitat suficient per atendre els diferents serveis plantejats en aquest plec. Per aquest servei recurrent el Plec de Clàusules Administratives (PCAP) determina un import durant el termini del contracte que s'executarà d'acord amb les prestacions que el licitador assoleixi.

3.4.2 Serveis variables

En relació amb els serveis inclosos en la present licitació, l'Agència estableix la possibilitat de dur a terme actuacions addicionals o projectes de caràcter excepcional, la volumetria dels quals no es pot preveure ni concretar en el moment d'elaborar aquest plec.

Aquesta prestació variable no està sotmesa a l'obligatorietat de la seva realització sinó que s'utilitzarà en funció de les necessitats de l'Agència. Aquestes prestacions dependran de que, si s'escau, es rebi la petició efectiva a l'Agència per a dur a terme

la prestació de serveis, que es disposi de la partida econòmica necessària per a dur a terme la seva execució i, de que el licitador ofereixi una solució competitiva en el moment en què es sol·liciti la seva participació. Serà l'Agència qui sol·licitarà al licitador, durant l'execució del contracte, una valoració d'esforç per a dur a terme aquestes tasques definides com a variables (definint, en tot cas, la necessitat) i, en cas que la valoració acompleixi els requisits d'adequació i competitivitat, l'Agència podrà sol·licitar l'execució de les mateixes a l'adjudicatari. En cap cas serà obligatòria la prestació mitjançant els serveis de l'adjudicatari quedant a discreció de l'Agència aquesta prestació segons els criteris establerts per al servei.

La definició dels serveis inclosos en aquesta categoria és subjecta a la proposta de serveis que el licitador formuli per als serveis recurrents d'aquest contracte (ja que són de la mateixa naturalesa) i, per tant, es valoraran amb la proposta de serveis recurrents. Sens perjudici de fer-ho voluntàriament, **no serà necessari doncs que el licitador proposi una solució específica** per aquests serveis variables sinó que es prendrà com a referència la descripció de serveis feta.

3.5 Gestió del servei

La capa de gestió de servei ha de concentrar les funcions destinades a facilitar el funcionament del servei, la coordinació dels recursos i la gestió i comunicació operativa, tàctica i estratègica amb l'Agència. Aquestes tasques s'han de realitzar seguint metodologies internacionalment reconegudes, com ara ITIL, que optimitzin els processos que es realitzen.

De la mateixa manera, aquesta capa, serveix com a vincle entre la direcció i l'operativa, adaptant el llenguatge tècnic propi de l'operació a un més orientat a negoci que aporti informació de valor a la direcció.

D'aquesta manera es defineixen algunes de les activitats a desenvolupar des d'aquesta capa de Gestió:

- Lideratge del seguiment d'activitats recollits en l'àmbit d'actuació del servei, assegurant la seva correcta planificació, priorització i acompliment de fites i funcions.
- Gestió i control de la informació (KDB) dels processos operatius que suporten les activitats del servei, incloent tant procediments com instruccions operatives.
- Definició, millora i manteniment de procediments i instruccions operatives del propi servei, així com altres de caire més transversal - acordats amb el responsable del servei - que facilitin la coordinació entre els diferents equips del SOC/CERT.

- 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.
- Coordinació amb la resta d'àrees i equips de l'Agència de Ciberseguretat.
- Integració de l'operativa amb tercers necessaris pel desenvolupament de la funció (per exemple, entre d'altres: RSIs, Àrea de Govern de la Dada, CTTI, AOC, hospitals i negoci).
- Suport a la resolució de conflictes i incidències operatives dins del propi servei o vinculades a la relació del servei del contracte amb altres serveis de l'Agència.
- Consolidació i aportació a l'Agència de les informacions objectives i subjectives que permetin a la Direcció la presa de decisions operatives, tàctiques i estratègiques relacionades amb el contracte.
- Gestió de la capacitat del servei, incloent entre d'altres: la coordinació dels perfils assignats davant de possibles rotacions de l'equip, mesura del grau de capacitat en base a les funcions acordades, i adequació o redimensionament/redistribució dels esforços segons prioritats del servei.
- Implementació de processos de traspàs de coneixement per atendre possibles rotacions dins de l'equip del servei.
- Garantia de qualitat del servei.
- Gestió de riscos operatius del servei.
- Disseny i presentació d'un "Pla de Transformació", basat en la identificació d'oportunitats de millora i evolució del servei.

Addicionalment, amb independència del model organitzatiu proposat, i com suport essencial per aquesta capa de gestió, el licitador haurà de designar com a mínim una persona a actuar com a **Cap de Servei**, que serà el principal responsable del servei, encarregat de dirigir i gestionar la relació del contracte i el servei de l'adjudicatari amb l'Agència. A aquest efecte, aquest rol ha d'assumir les següents responsabilitats:

- Actuar com a punt de contacte únic en relació amb la gestió ordinària del servei de l'adjudicatari amb poder de decisió sobre els principals elements del contracte.
- Actuar com a principal punt de coordinació amb el Responsable de la Línia de Servei (RLS) de l'Agència de Ciberseguretat, per tal de garantir la correcta execució de les capes de gestió, administració i servei.

- Consolidar i aportar a l'Agència les informacions objectives i subjectives que permetin a la Direcció de l'àrea la presa de decisions operatives i estratègiques relacionades amb el contracte i els serveis que se suporten.
- Garantir que l'Agència rebi els informes de gestió acordats i realitzar el seguiment econòmic i d'activitat amb els interlocutors de l'Agència.
- Garantir la transparència en el control de gestió per tal d'agilitzar el procés de seguiment i facturació.
- Coordinar i fer el seguiment de l'activitat.
- Gestionar la capacitat del servei, la seva disponibilitat i mantenir la informació al respecte (vacances, torns, rotació, manca o ampliació de recursos, etc.).
- Controlar i gestionar els plans de formació i de traspàs de coneixement del personal assignat al servei.
- Assegurar una bona col·laboració entre els diferents agents implicats en la prestació de serveis a l'Agència.

Per altra banda, el licitador també designarà un **coordinador** per tal garantir la correcta **gestió operativa del contracte**, així com del desplegament i evolució tàctica, per tal de que aquest estigui alineats amb els objectius estratègics de l'Agència de Ciberseguretat. Aquest coordinador, serà l'interlocutor amb qui treballar periòdicament amb el Director de l'àrea del Centre d'Operacions de l'Agència de Ciberseguretat (SOC/CERT) i el RLS corresponent.

Es valorarà la proposta del licitador per disposar dels perfils de cap de servei i coordinador, adaptats dins d'un model orientat a servei, no a persones, on no es requereix obligatòriament presencialitat física pel servei de suport licitat.

El licitador ha d'incloure en la seva proposta un model de govern que: (i) garanteixi que el cap de servei lideri l'estratègia de desplegament del servei, a més, i (ii) la resta de membres de l'equip identifiqui de forma clara el rol de gestió del servei.

3.6 Millora dels serveis

Amb l'objectiu d'augmentar el nivell de maduresa del servei i els seus subserveis, així com millorar l'eficiència de l'activitat operativa en el temps, especialment amb totes les tasques que es realitzin en estreta col·laboració amb la resta de serveis o accions executades a fi d'evolucionar la prestació dels serveis de l'Agència de Ciberseguretat, els licitadors hauran de contemplar una part de l'esforç (que ha de dedicar el mateix licitador) amb aquesta finalitat.

Alguns exemples a tenir en compte són:

- Millora de la metodologia de treball del servei.
- Millora dels productes a lliurar.
- Reducció dels temps de les tasques a realitzar.
- Optimització de les eines de treball.
- Millora de mètriques i indicadors operatius.
- Industrialització i automatització de processos.
- Millora d'eficiència i eficiència de processos, tecnologies, etc.

Totes les tasques de transformació seran sempre acordades, planificades i validades prèviament d'acord al nivell d'evolució i millora que aportin al servei.

3.7 Equip de treball i perfils

3.7.1 Equip humà

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos humans propis de l'adjudicatari (o subcontractistes autoritzats) amb la qualificació necessària i adequada per a la prestació del servei.

Els mitjans personals necessaris per a la prestació dels serveis anteriorment indicats han de ser els adequats per realitzar amb garanties 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 e 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 tecnològic i de negoci de seguretat informàtica i de l'entorn de l'administració pública.

L'adjudicatari haurà de presentar un plantejament organitzatiu dimensionat pels diferents grups que composen el contracte, que asseguri la cobertura de les funcions que s'han descrit al present Plec i permeti mantenir un model de relació fluid amb la resta d'equips i personal de l'Agència.

L'Agència tindrà dret a exigir justificadament a l'adjudicatari 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. L'adjudicatari haurà de presentar en un termini màxim de 10 dies 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. Aquesta substitució no podrà superar el termini de 15 dies a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència al cap de servei.

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 dels personal que donen servei a l'Agència evitant, sempre que sigui possible, la rotació del perfil corresponent al **cap de servei, així com aquells que desenvolupin tasques rellevants en la prestació de serveis (coordinadors de servei, persones clau en la prestació, etc.).**

Les hores dedicades pel personal de l'adjudicatari a la transició i/o formació del personal sortint i entrant en cas de substitució no es podrà facturar. S'acordarà entre l'adjudicatari i l'Agència el temps estimat de transició per cada substitució que es produeixi, essent el **període mínim establert per a la transició de 4 dies laborables**.

Quan la rotació sigui necessària (baixes, canvis de perfil, etc.) l'adjudicatari haurà d'acreditar la idoneïtat del nou personal prèvia incorporació dels nous recursos. En els casos de rotació ordinària i previsible (vacances, permisos laborals, etc.) l'adjudicatari comunicarà a l'Agència amb la deguda antelació un pla de substitució i disposició de recursos que doni resposta a les necessitats de l'Agència en la seva prestació de serveis durant els esmentats períodes.

Tenint en compte que l'objectiu de transformació i industrialització dels serveis a prestar ha de permetre a l'adjudicatari (i per tant a l'Agència) donar un nivell creixent de qualitat i volumetria de servei amb els mateixos recursos, **el nombre mínim d'hores efectives anuals necessàries** per l'execució dels serveis demanats en aquest plec és la següent:

LOT 1 – Governança de l'Operació del SOC/CERT: Subserveis	Hores mínimes anuals
Gestió de la Demanda	3.560 h/any
Resta de serveis de Governança de l'operació del SOC/CERT	3.560 h/any

LOT 2 - Gestió de Projectes i Pla d'Evolució	Hores mínimes anuals
Gestió de projectes i Pla d'Evolució	7.120 h/any

LOT 3- Arquitectura de seguretat i evolució de solucions	Hores mínimes anuals
Arquitectura de seguretat i evolució de solucions	7.120 h/any

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

A nivell orientatiu, la distribució d'esforços que s'ha pres de referència per la configuració de la present licitació ha estat la següent:

LOT 1 - BLOC DE SERVEI	DISTRIBUCIÓ ORIENTATIVA
Gestió de la demanda	50%
Govern de l'operativa	25%
Entrega de valor	15%
Gestió del coneixement	10%

LOT 2 - BLOC DE SERVEI	DISTRIBUCIÓ ORIENTATIVA
Gestió de projectes	90%
Pla d'Evolució	10%

LOT 3 - BLOC DE SERVEI	DISTRIBUCIÓ ORIENTATIVA
Arquitectura de seguretat	25%
Evolució de solucions	75%

La oferta haurà de detallar la proposta de distribució d'esforços segons consideri d'acord amb el model de govern i objectius del servei.

3.7.2 Perfils

A continuació es presenten els requeriments valorables dels perfils professionals que compondran els equips.

3.7.2.1 Lot 1 – Governança de l'operació del SOC/CERT

Perfil	Requisits
Gestor/Cap del Servei	• Experiència professional mínima de 5 anys en gestió i lideratge de projectes i equips de serveis de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Coneixements en: ▪ Definició i millora de processos. ▪ Eines de *reporting* i quadres de comandament. ▪ Tecnologies aplicades a centres d'operació de la seguretat (SOCs). ▪ Marcs metodològics més comuns de gestió (ITIL, ISO 20000, Prince2, COBIT, PMP o similar) i de seguretat (ISO27000, NIST o similar)
Consultor de seguretat	• Experiència professional mínima de 3 anys en projectes de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Haver participat i poder demostrar la seva involucració en mínim un projecte en els que hagi desenvolupat les següents funcions: ▪ Lideratge de projectes i equips de treball multidisciplinars. ▪ Gestió i operació de serveis de SOC. ▪ Definició de Plans Directors de Seguretat. ▪ Anàlisi de riscos de seguretat i propostes de plans d'acció correctius. ▪ Elaboració d'informes executius, incloent la definició i implantació de quadres de comandament, els quals incorporen visions estratègiques, operatives i tàctiques. ▪ Gestió de projectes de seguretat. ▪ Definició i desplegament de processos de gestió de la seguretat. ▪ Definició, implantació i automatització d'indicadors de servei, especialment en l'àmbit de la ciberseguretat. • Coneixements en: ▪ Definició de projectes (metodologies, processos, eines, lliurables, etc.). ▪ Eines de BI, especialment Microsoft PowerBI. ▪ Eines de generació i presentació d'informació per fer més eficient la comunicació i presa de decisions. ▪ Principals vulnerabilitats i defectes a les que poden estar subjectes infraestructures, plataformes i aplicacions (Desbordaments de memòria, Injeccions de codi, errors d'autenticació i autorització, implementacions criptogràfiques

Perfil	Requisits
	incorrectes, gestió deficient d'errors i excepcions etc.) així com les propostes de mitigació cost/efectivitat més adients. ▪ Principals amenaces i vectors d'atac que afecten a les organitzacions (per exemple, el catàleg d'amenaces que proposa l'organització NIST). • Habilitats comunicatives avançades i capacitat de coordinació i interlocució amb altres equips.
Tècnic de suport a la gestió de la demanda i comitès de crisis	• Experiència professional mínima de 3 anys en l'atenció i gestió de peticions de clients, així com la gestió administrativa i acompanyament a altres funcions en esdeveniments rellevants (p.ex. comitès de crisi). • Titulació en l'àmbit tecnològic actual (incloent formació professional, cicles formatius i altres) que l'habiliti a realitzar les funcions requerides: ▪ Gestió d'eines de tiqueting (OTRS, Jira, Remedy, HP ServiceManager) ▪ Atenció al client ▪ Seguiment administratiu de peticions, formularis, etc. ▪ Interlocució amb equips de treball multi-disciplinar, usuaris clau i usuaris d'alt nivell. ▪ Suport i coordinació en la gestió de crisis i gestió de conflictes ▪ Suport administratiu en la planificació i formalització d'actes de reunions. • Addicionalment, ha de tenir les següents aptituds mínimes: ▪ Capacitat per l'execució de tasques procedimentades. ▪ Comunicació interpersonal ▪ Lideratge i proactivitat ▪ Habilitats comunicatives i dots de mediació en funció dels destinataris ▪ Capacitat de síntesis ▪ Capacitat d'adaptació ▪ Empatia i alta capacitat d'anàlisi davant situacions crítiques o d'elevada pressió. • Coneixements en: ▪ IT i ciberseguretat bàsica, per facilitar l'atenció i gestió de les peticions responsabilitat del SOC/CERT. ▪ Estàndards com ISO 22320, ISO 22361, per facilitar l'atenció i gestió de situacions de crisis

3.7.2.2 Lot 2- Gestió de Projectes i Pla d'Evolució

Perfil	Requisits
Gestor/Cap del Servei	• Experiència professional mínima de 5 anys en gestió i lideratge de projectes i equips de serveis de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Coneixements en: ▪ Definició i millora de processos. ▪ Eines de *reporting* i quadres de comandament. ▪ Tecnologies aplicades a centres d'operació de la seguretat (SOCs). ▪ Marcs metodològics més comuns de gestió (ITIL, ISO 20000, Prince2, COBIT, PMP o similar) i de seguretat (ISO27000, NIST o similar).
Gestor de Projectes	• Experiència professional mínima de 3 anys en gestió de projectes. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Haver participat i poder demostrar la seva involucració en mínim un projecte en els que hagi desenvolupat les següents funcions: ▪ Lideratge de projectes i equips de treball multidisciplinars. ▪ Gestió i seguiment de projectes (incloent la identificació i validació de requeriments, gestió de riscos, identificació i control de desviaments de terminis, etc.) • Coneixements en: ▪ IT i ciberseguretat bàsica ▪ Eines de *reporting* i quadres de comandament. • Mínim una certificació de gestió de projectes (per exemple: PMP, Scrum o similar).
Consultor de seguretat	• Experiència professional mínima de 3 anys en projectes de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Participació en com a mínim un projecte de disseny de plans directors de seguretat, anàlisi de riscos de seguretat i propostes de plans d'acció correctius, i elaboració d'informes executius • Coneixement en: ▪ IT i ciberseguretat bàsica ▪ Eines de generació i presentació d'informació per fer més eficient la comunicació i presa de decisions. ▪ Definició de projectes (metodologies, processos, eines, lliurables, etc.).

3.7.2.3 Lot 3 – Arquitectura de seguretat i Evolució de solucions

Perfil	Requisits
Gestor/Cap del Servei	• Experiència professional mínima de 5 anys en gestió i lideratge de projectes i equips de serveis de ciberseguretat. • Titulat universitari en Informàtica, Telecomunicacions o similars en l'àmbit TI. • Coneixements en: ▪ Definició i millora de processos. ▪ Eines de *reporting* i quadres de comandament. ▪ Tecnologies aplicades a centres d'operació de la seguretat (SOCs). • Marcs metodològics més comuns de gestió (ITIL, ISO 20000, Prince2, COBIT, PMP o similar) i de seguretat (ISO27000, NIST o similar)
Arquitecte de seguretat	• Experiència professional mínima de 3 anys en el món de la seguretat informàtica. • Titulació universitària en Enginyeria en informàtica, telecomunicacions o similars en l'àmbit TI. • Participació en com a mínim un projecte on hagi desenvolupat les següents funcions: ▪ Disseny i desplegament d'infraestructura de seguretat: Checkpoint, Palo Alto, CISCO, McAfee, Symantec, Crowdstrike, Fireeye, Radware, entre d'altres. ▪ Operació i administració d'eines de ciberseguretat com a part d'un equip SOC/CERT. ▪ Projectes en entorns multi-proveïdor. ▪ Gestió de *logs* en entorns complexes i grans. ▪ Avaluació i gestió de riscos de seguretat. ▪ Desenvolupament de projectes i sistemes d'informació. • Coneixement en: ▪ Governança i definició de millors pràctiques d'arquitectures de seguretat. ▪ Arquitectures estàndard dels principals fabricants com: IBM, CISCO, Splunk, Crowdstrike, Palo Alto, Microsoft, Cloud Computing (Azure, Amazon Web Services, Office 365, Oracle…), Weblogic, SAP, Atlassian (JIRA, Confluence, etc.) ▪ Definició de projectes (aproximacions i processos, eines, lliurables, etc.). ▪ Tendències tecnològiques, fabricants, estratègies de productes i fulls de ruta. ▪ Estàndards i metodologies corporatives (p.e: ITIL, ISO 27001, PMP, etc.) ▪ Sistemes de seguretat tant tradicionals com emergents (Per exemple: WAF, Proxies i Filtrat de continguts, IPS, Firewalls, Routers i switchos, VPN, VRF, sistemes d'encriptació, DNS, DDOS, IPv4 i IPv6, sistemes d'autenticació de múltiple factor, PKI's, DLP, Gestió de logs, sistemes de protecció del lloc de treball, etc.

Perfil	Requisits
	▪ Principals vulnerabilitats i defectes a les que poden estar subjectes infraestructures, plataformes i aplicacions (Desbordaments de memòria, Injeccions de codi, errors d'autenticació i autorització, implementacions criptogràfiques incorrectes, gestió deficient d'errors i excepcions etc.) així com les propostes de mitigació cost/efectivitat més adients. • Nivell alt o mitjà d'anglès.
Desenvolupador	• Experiència professional mínima de 2 anys en el món de la seguretat informàtica. • Titulació universitària en Enginyeria en informàtica, telecomunicacions o similars en l'àmbit TI. • Participació en com a mínim un projecte on hagi desenvolupat alguna de les següents funcions: ▪ Automatització de tasques operatives recurrents. ▪ Desenvolupament i consum d'APIs. ▪ Disseny pixel-perfect i responsive ▪ Desenvolupament full *stack* multi plataforma. ▪ Implementació i administració de casos d'ús i *playbooks* i automatitzacions en eines SIEM/SOAR (Splunk i XSOAR preferiblement) ▪ Desenvolupament de Backend WEB y API REST • Coneixement en: ▪ *Scripting* per a la automatització de tasques operatives recurrents. ▪ Llenguatges de programació més comuns (per exemple Python, JavaScript, etc.) ▪ Estàndards bàsics de programació (MVC, patrones de disseny, modularització, re usabilitat, TDD, etc). ▪ Bones pràctiques en consideracions d'accessibilitat, estàndards web actuals i experiència d'usuari. ▪ Eines de desenvolupament i col·laboració: GIT, JIRA. ▪ Desenvolupament seguint metodologies *Agile*. • Nivell alt o mitjà d'anglès.

3.8 Idioma del servei

Seguint les indicacions de la LLEI 1/1998, de 7 de gener, de política lingüística, l'idioma de prestació dels serveis cap a l'Agència i cap als seus clients haurà de ser Català, així com l'emprat a la documentació que l'adjudicatari generi durant la prestació del servei cap als seus clients, sens perjudici del dret dels ciutadans i ciutadanes a rebre-les en Castellà, si ho demanen. En el cas de la comunicació amb la resta dels equips que composen el SOC/CERT, l'idioma podrà ser el Català, el Castellà o l'Anglès.

3.9 Eines

L'Agència disposa de diverses eines/repositoris que permeten per una banda, als equips de l'Agència desplegar els seus serveis, i per altra, donar una visió clara dels resultats de la seva activitat així com establir plans d'acció i millora. Concretament, les principals eines i repositoris a l'Agència que serien aplicables a aquest contracte són:

- **Eina de *ticketing* per la gestió de casos i peticions dirigit als serveis del SOC/CERT** (actualment OTRS).
- **Eina de *ticketing* per la gestió de casos i peticions dirigides a CTTI** (Actualment Remedy).
- **Repositori d'informació del SOC/CERT (INFOSOC)**, utilitzada per tots els serveis del SOC/CERT per registrar i creuar dades útils per l'operació de la seguretat.
- **Gestor documental (Confluence)** com a repositori de lliurables, documentació dels processos i procediments del servei i altra informació estàtica útil per la operació dels serveis.
- **Eina de presentació d'indicadors** (actualment Microsoft Power BI).
- **Eina Kanban d'orquestració** (actualment JIRA).
- **Eina de treball col·laboratiu** (actualment Microsoft Teams).

Els licitadors del contracte objecte d'aquest expedient hauran de:

- Operar les eines actuals i futures, d'acord els estàndards vigents de l'Agència.
- Formar i certificar (si s'escau) a l'equip operatiu en totes les eines que l'Agència disposa que siguin requerides per part de l'adjudicatari pel normal funcionament del servei.
- Garantir que totes les comunicacions/interaccions amb altres persones es realitzen utilitzant els comptes de servei habilitats a les eines de seguiment de l'activitat (per exemple, eines de gestió de l'activitat mitjançant tiquets).
- Gestionar el servei i definir en tot moment els requeriments i necessitats de manteniment de les eines de gestió (de projectes, de sistemes, de rendiment, de disponibilitat, etc.) que l'Agència de Ciberseguretat de Catalunya posi a la seva disposició en cada moment.
- Proposar millores i si s'escau per la prestació del servei aportar-ne de noves.

En el cas en què el licitador ho consideri necessari podrà plantejar la incorporació de noves eines per desenvolupar les seves funcions, explicant amb detall com les noves eines donen valor al servei i a l'Agència, sempre tenint en compte els objectius de celeritat en la prestació dels serveis, així com la d'aprofitar sinèrgies i eficiències

econòmiques. En aquest cas, es valorarà positivament que les eines proposades per a incorporar a l'Agència siguin "de mercat" en lloc de propietàries.

És de vital importància que les eines s'integrin no només amb el servei específic, sinó també amb la resta d'eines dels diferents serveis, ja que els serveis i els seus processos es necessitaran mútuament.

Donada la segmentació en els àmbits de responsabilitat dins de l'estructura organitzativa de l'Agència, s'ha de tenir en compte que l'esperit general en referència a les eines i sistemes d'informació és que l'adjudicatari serà l'encarregat de proporcionar i instal·lar les noves eines (el cost d'instal·lació haurà d'estar previst com una part més del cost de les eines), que l'equip de Mitjans Tècnics de l'Agència s'encarregarà sempre del seu desplegament, manteniment i operació tècnica (copies, rotació de *logs*, control de la infraestructura, etc.) i els equips dels altres blocs organitzatius s'encarregaran de la parametrització (per l'adequació a l'ús segons les seves necessitats puntuals en cada moment) i potencialment de l'ús d'aquestes eines.

Aquest document inclou indicacions de com es pot accedir al llistat actualitzat d'eines específiques disponibles dins de l'Agència (veure apartat 6. ANNEX I – LLISTAT D'EINES).

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.

Finalment, indicar que el licitador no podrà extreure informació de cap eina fora de l'àmbit d'actuació per la seva manipulació o explotació sense autorització prèvia de l'Agència.

3.10 Infraestructura i equipament per la prestació dels serveis

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

- Ubicació física adequada per al desenvolupament i prestació del servei, a les instal·lacions de l'Agència.
- Accés a Internet a través de la xarxa 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.
- 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.

Addicionalment, independentment de la modalitat de prestació del servei (en remot o presencial), l'Agència proveirà de:

- Telefonia mòbil per donar cobertura als serveis de guàrdia.
- Correus electrònics i eines ofimàtiques i col·laboratives Suite O365.
- Llicència Microsoft PowerBI per 1 o 2 membres de l'equip.

L'Agència no proveirà:

- Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina.
- 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.

Per aquells serveis que impliquin una prestació continuada i la necessitat d'accedir a la infraestructura tecnològica de l'Agència, l'Agència proporcionarà a l'adjudicatari:

- Ordinadors portàtils amb el programari habitual de l'Agència per a la prestació del servei.
- Les eines lligades al lloc de treball necessàries per a la prestació del servei. **Cost mínim orientatiu de la llicencia bàsica i maquinari és de 585€ anuals per lloc de treball que es repercutirà a l'adjudicatari. En cas que es requereixin per a la prestació del servei altres llicències no bàsiques, les podrà aportar l'adjudicatari amb el vist-i-plau de l'Agència, o bé proporcionar-les l'entitat, tot compensant els costos que aquest fet generi.**

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 "Lloc de Treball" de l'Agència.

3.11 Seguretat Corporativa

Tant l'empresa adjudicatària com el personal de l'adjudicatari 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.

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

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

3.12 Govern de la dada i govern del risc

Tots els serveis de l'entitat generen, actualment, un elevat nombre d'indicadors derivat de l'execució dels serveis de l'entitat en aplicació dels seus processos, procediments i protocols específics de cada servei, que cal mantenir i evolucionar constantment per part de l'adjudicatari.

En concordança amb la resta de serveis de l'Agència, la generació d'aquests indicadors s'integra amb el Repositori de Indicadors de Servei de l'Agència (RICA), i posteriorment es visualitzen en eines que faciliten la gestió dels mateixos, com ara eines de tipus BI (Power BI). Aquest procés de càrrega i visualització dels indicadors recollits en RICA, és funció del servei de Govern de la Dada de l'Agència, amb el que l'adjudicatari s'ha de coordinar contínuament per garantir una correcta càrrega dels indicadors establerts, i l'evolució dels mateixos.

El format de generació dels indicadors del servei, depèn de la naturalesa dels mateixos (*logs*, registres propis, extraccions d'altres BBDD, etc.), i del tractament que el servei hi aplica per extreure'n la informació en format indicador.

Aquests indicadors propis del servei, són proposats, desenvolupats, generats i mantinguts pel servei i acordats amb el Responsable de Línia de Servei i s'hauran de reportar periòdicament (com a molt en períodes mensuals) al Responsable de Línia de Servei per al seguiment del mateix. Si no es tracten directament amb les eines i repositoris indicats anteriorment, s'hauran de generar i processar amb eines compatibles amb les previstes per l'Agència de Ciberseguretat de Catalunya, sempre amb previ acord del Responsable de Línia de Servei.

Així mateix, el licitador haurà d'elaborar, mantenir i reportar els indicadors d'activitat al Director de l'àrea en la qual es trobi el servei en qüestió. Aquests indicadors d'activitat seran detallats en les diferents reunions de seguiment de servei i versaran respecte de l'estat d'execució dels serveis, la dedicació de recursos per servei, la capacitat prevista, els ratis d'eficiència derivats de l'activitat i els processos de millora, entre d'altres. Aquests indicadors podran ser proposats pel licitador tant en la mateixa oferta com durant l'execució del contracte al Director de l'àrea corresponent que els haurà d'acceptar per la seva implantació i seguiment.

3.13 Control de la Gestió i Prestació de serveis

El personal del licitador, i en especial el cap del servei, haurà de col·laborar amb l'àrea de Control de Gestió de l'Agència per tal de:

- Definir un model de seguiment econòmic i planificació en termes de capacitat i execució de tasques.
- Ajustar-se als procediments de facturació que determini l'Agència.
- Conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència, d'acord amb els procediments establerts.
- 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
    - 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. **L'adjudicatari suportarà els costos d'auditories adjudicades a tercers i gestionades per l'Agència, destinant al seu finançament un màxim del 0.7% de l'import anual dels serveis contractats**.

3.14 Propietat i validació de la 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 responsables de cada línia de servei de l'Agència seran els responsables de la validació i aprovació dels documents elaborats pel personal de l'adjudicatari. En cas que la qualitat dels documents sigui molt baixa o de manera recurrent i/o perllongada en el temps de prestació dels serveis no assoleixi els nivells requerits s'aplicaran les penalitzacions establertes en la present licitació.

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

3.15 Integració amb altres equips

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

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 les altres àrees operatives de 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; a tall d'exemple, el descobriment d'una nova tendència en l'àmbit d'actuació dels serveis.

3.16 Formació

El personal de l'adjudicatari disposarà de la formació adequada per al desenvolupament de les seves tasques. Sens perjudici d'aquesta qüestió el personal de l'adjudicatari 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.

L'adjudicatari haurà de reservar un 5% del temps del personal per tasques de formació i certificació (en matèries relacionades amb l'activitat del contracte) i aquest temps no serà facturat a l'Agència ni tindrà impacte sobre el pla de capacitat del servei, valorant-se la disposició d'un pla de capacitació del personal de l'adjudicatari destinat a l'Agència. Aquest pla es coordinarà amb les activitats i accions de formació pròpies de l'Agència.

3.17 Contingència

Els licitadors hauran de contemplar les mesures de contingència que considerin oportunes per tal d'assegurar el mínim impacte possible en la prestació del servei davant de qualsevol desastre inesperat, independentment del format de la seva prestació (ja sigui presencial o en remot).

4 ACORDS DE NIVELL DE SERVEI I PENALITZACIONS

L'adjudicatari resta obligat al compliment de l'execució total de les prestacions recollides en les ofertes que acompleixi al present plec i a les prescripcions del contracte. Així mateix, l'adjudicatari haurà de disposar d'un cronograma que permeti definir els terminis parcials de compliment en la prestació de serveis d'acord amb l'apartat de planificació.

Així mateix la prestació de serveis de l'adjudicatari haurà de complir uns estàndards de qualitat mínims que permetin fer-ne un aprofitament adequat i donin resposta a les necessitats de l'Agència. En cas que els serveis no assoleixin aquests mínims de qualitat requerits es considerarà l'existència d'un incompliment d'acord amb el model recollit en aquest apartat.

A continuació es descriu el model de penalitzacions que s'aplicaran per l'incompliment dels indicadors i Acords de Nivell de Servei ("ANS") definits, d'acord amb els criteris, quantificació i mètode de càlcul establerts més endavant, entenent que un mateix fet pot donar lloc a l'aplicació de diferents incompliments i les corresponents penalitzacions d'igual o diferent tipus.

La imposició de penalitzacions i la facultat resolutòria de l' Agència per incompliment es regiran per l'establert als articles 192 i següents de la LCSP.

En cap cas les penalitzacions tindran finalitat recaptatòria, de manera que la seva aplicació no substituirà ni minorarà la indemnització que per danys i perjudicis pogués resultar dels corresponents incompliments.

4.1 Models de mesura del nivell de servei

Per tal de disposar de la informació necessària per a una gestió i governança homogènia l'Agència defineix un Model de Mesura del Nivell de Servei que ha de permetre la valoració dels Acords dels Nivells de Servei (ANS) i la seva millora contínua.

L'Agència implantarà el Model de Mesura del Nivell de Servei de forma progressiva al llarg de l'execució del contracte. En aquest sentit, l'adjudicatari i l'Agència acordaran la estratègia per implementar els respectius ANS en cada un dels àmbits d'actuació.

El licitador ha d'incloure una planificació pel desplegament del 100% del model de mesura dels Acords dels Nivells de Servei a tots els àmbits d'actuació de l'Agència de Ciberseguretat. Es valorarà positivament una proposta que permeti desplegar amb garanties el model complert, reduint els temps requerits per aconseguir-ho.

El licitador inclourà també a la seva proposta la llista d'informes de seguiment del servei i del contracte que generarà, indicant el seu contingut, periodicitat, fonts d'informació, i qualsevol altra dada que consideri rellevant.

Li correspon a l'adjudicatari presentar mensualment, com a part del conjunt d'informes de seguiment del servei, un report amb la valoració del compliment de tots els nivells de servei i indicadors de mesura que s'especifiquen a continuació en aquest apartat. La qualitat i exactitud d'aquest informe són claus per a un bon control del servei i per mantenir una bona relació entre l'Adjudicatari i l'Agència.

El licitador haurà d'incloure dintre de la seva oferta una proposta dels principals indicadors que, en funció del seu enteniment, permeten mesurar de la forma més adient el valor presentat pel servei inclòs en la present licitació, així com la millora dels proposats en els següents apartats.

Aquests indicadors hauran d'incorporar una definició específica de cadascun d'ells així com la formula de càlcul aplicable.

4.2 Model de penalitzacions pels serveis

El licitador s'haurà d'ajustar al model penalitzacions que a continuació es descriu i que inclou els següents punts:

- Càlcul de les penalitzacions
- Aplicació de les penalitzacions
- Irregularitats en les mesures
- Incompliment de la normativa interna de l'Agència

Les penalitzacions s'aplicaran per incompliment dels Nivell de Servei indicats en la taula d'Acords de Nivell de Servei.

El càlcul de l'import de la penalització es fa seguint les indicacions del Plec de Clàusules Administratives.

4.2.1 Incompliment de la normativa interna de l'Agència

Tal i com s'ha exposat anteriorment en el present plec l'Agència disposa de normativa reguladora en matèria de seguretat corporativa i de protecció de la seva informació. L'incompliment d'aquesta normativa pot implicar greus perjudicis a l'Agència i, per tant, s'estableix un sistema particular de penalitzacions vinculades al respecte a aquesta normativa per part dels licitadors. Aquest sistema de penalitzacions en cap cas té voluntat recaptatòria sinó que té com a finalitat promocionar el compliment de la seva normativa interna per part dels licitadors i les persones que efectivament presten els serveis.

L'Agència aplicarà una penalització per un import d'un tant alçat d'entre 50€ i 100€ per cada incompliment de la normativa vigent en matèria de seguretat corporativa i normativa interna que realitzi l'adjudicatari i el personal que aquest aporti (incloent el personal que pugui aportar en subcontractacions sota la seva responsabilitat). La graduació de l'import es produirà, atenent a la gravetat, continuïtat de la infracció, duració, intensitat, grau de risc que hagi causat la infracció, entre d'altres. En cap cas aquesta penalització limitarà la capacitat de l'Agència de reclamar els danys i perjudicis efectivament causats per l'incompliment d'acord amb el contracte vigent entre les parts.

L'òrgan responsable de determinar l'existència d'una infracció serà el cap de seguretat corporativa de l'Agència qui un cop detectat un presumpte incompliment ho notificarà per correu electrònic a la persona responsable de l'adjudicatari i donarà un termini raonable per a que l'adjudicatari al·legui el que consideri en el seu interès. Veient la informació disponible i les condicions corresponents al cas, el responsable de seguretat corporativa determinarà i notificarà definitivament l'existència d'un incompliment de la normativa i notificarà la imposició de la penalització de manera

definitiva a l'adjudicatari. El procediment de facturació de les penalitzacions es regula per l'apartat "**Error! No s'ha trobat l'origen de la referència.**. Facturació de les penalitzacions".

4.2.2 Taula d'indicadors subjectes a acords de nivells de servei

4.2.2.1 Bloc de servei Lot 1: Governança de l'operació del SOC/CERT

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
Personal						
GESPER01	Rotació de Personal	Índex de rotació del personal en el servei (queden excloses d'aquest indicador les admissions i les desvinculacions per variació del nombre d'efectius del servei per possible modificació del nombre d'efectius del servei recollida en la proposta de servei)	Índex de rotació de personal [%] Càlcul = ((admissions de personal + desvinculacions de personal)/2) *100) / (nombre d'efectius del servei pel període considerat)	Mensual	N/A	% de rotació per l'import de la factura del període
GESPER02	No disponibilitat de Personal	Incompliment de l'horari de servei, la no disponibilitat de servei o la no presència en el lloc de treball del personal en qualsevol moment del període contractat.	Hores d'incompliment de servei [h] Càlcul = Total d'hores de falta de presència d'un perfil durant l'horari de servei acordat amb l'Agència. Nota: Es considerarà l'arrodoniment a l'alça (nombre sencer en hores) de la suma acumulada dels períodes de no disponibilitat. (Per exemple, 35 min es considerarà com 1 hora a efectes de penalització o 2 hores i 20 minuts com 3 hores)	Mensual	N/A	Import de 2h de servei per cada hora d'indisponiblitat.
GESPER03	Falta de substitució de perfils	Faltes de substitució de personal quan es produeix una desvinculació.	Hores amb manca de substitució [h] Càlcul = Total d'hores de falta de presència degut a una desvinculació prèvia.	Mensual	N/A	Descompte de la meitat d'hores del perfil desvinculat en el contracte del servei.
Qualitat						
GESQUA01	Qualitat dels lliurables del servei	Grau de satisfacció de l'Agència respecte la qualitat i contingut dels lliurables generats pel	Puntuació [de 1 (menys satisfactori) a 10 (més satisfactori)] segons enquestes de	Mensual	6	5% de l'import de la facturació del període

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
		servei. Entre d'altres, els aspectes més importants definits als apartats "Lliurables del servei" i "Mètriques i indicadors".	satisfacció al responsable del servei de l'Agència. Nota: El contingut de les enquestes ha de ser acordat previ a la fase de prestació del servei.			
GESQUA02	Qualitat la prestació del servei	Grau de satisfacció de l'Agència respecte la prestació del servei en general, valorant entre d'altres: dedicació i rendiments del perfils assignats, assoliment de fites, incidències amb el servei, compliment de procediments/fluxos definits, etc.	Puntuació [de 1 (menys satisfactori) a 10 (més satisfactori)] segons enquestes de satisfacció al responsable del servei de l'Agència. Nota: El contingut de les enquestes ha de ser acordat previ a la fase de prestació del servei.	Mensual	6	5% de l'import de la facturació del període
GESQUA03	Compromís amb les dates d'entrega	Incompliment de les dates acordades d'entrega dels diferents lliurables (informes, mètriques, indicadors, etc.) o fites definides.	Nombre de lliurables-productes-fites a entregar en el mes, que no han sigut lliurats [N1] Nombre de lliurables-productes-fites entregats en una data posterior a l'acordada [N2], especificant el nombre de dies desviats respecte la data d'entrega establerta [d]. Nota: En cas que l'incompliment d'un termini estigui justificat per dependència de tercers caldrà aportar el raonament oportú.	Mensual	N1 >= 1 N2 >= 3	(N1 * (3% de l'import de la facturació del període)) + ((Suma de dies desviats) * (0,5% de l'import de la facturació del període))
Gestió documental						
GESDOC01	Manteniment de la informació rellevant del servei.	Nivell de revisió i manteniment dels procediments i instruccions operatives del servei. La disposició de documentació dels processos són clau per gestionar de manera efectiva les tasques del	Percentatge de documents actualitzats [%]. Càlcul = (Número de documents mensuals actualitzats) / (número documents mensuals a actualitzar) * 100.	Mensual	95%	5% de l'import de la facturació del període

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
		servei. Per aquest motiu, s'ha de disposar i mantenir actualitzada qualsevol documentació que permeti garantir el compliment dels processos interns del servei.	On el número de documents actualitzar mensualment haurà de ser calculat en base a la quantitat del total de documents operatius del servei acordats amb el responsable del servei.			
Gestió de la demanda						
GESDEM01	Temps de resposta inadequat per part del servei	Control del temps de primer resposta per part del servei en la gestió de qualsevol petició, consulta o notificació rebuda.	Per a casos dirigits al servei general de gestió de la demanda, Nombre de casos on el temps de gestió en primera instància superi els 30 minuts. [N1] Per a casos dirigits a altres funcions del servei, Nombre de casos on el temps de gestió superi 1 jornada laboral. [N2] Nota: No es contempla dins del temps de resposta del servei, la resposta que pugui generar automàticament l'eina de tiqueting. Per als casos que arribin fora de l'horari del servei, s'iniciaria la mesura dels temps de resposta a partir de l'inici del servei a la jornada següent.	Mensual	N1 >= 95% N2 >= 90%	5% de la facturació del període.
GESDEM02	Incidències generades per gestió lenta	Incidències ocasionades per la gestió inadequada de la demanda.	Nombre d'incidències amb impacte significatiu reportades al servei o al responsable del servei per la manca d'una resposta àgil o de qualitat. [N]	Mensual	N >= 1	5% de l'import de la facturació del període.
GESDEM03	Assistència a comitès de crisi	Control de les reunions en les que es demana assistència i gestió d'un comitè de crisi i no s'assisteix en temps.	Nombre de reunions arribant amb més de 5 minuts de retard. [N]	Mensual	N >= 1	2% de l'import de la facturació del període per cada incompliment.
GESDEM04	Manca de gestió de comitès de crisis	Control dels comitès de crisi que hauria d'organitzar el servei.	Nombre de comitès de crisis no convocats en temps i forma per	Mensual	N >= 1	10% de l'import de la facturació del període per cada incompliment.

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
			la gestió d'incidents de seguretat. [N]			

4.2.2.2 Bloc de servei Lot 2: Gestió de projectes i Pla d'Evolució

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
Personal						
PEVPER01	Rotació de Personal	Índex de rotació del personal presencial en el servei (queden excloses d'aquest indicador les admissions i les desvinculacions per variació del nombre d'efectius del servei per possible modificació del nombre d'efectius del servei recollida en la proposta de servei)	Índex de rotació de personal [%] Càlcul = ((admissions de personal + desvinculacions de personal presencial)/2) *100) / (nombre d'efectius del servei pel període considerat)	Mensual	N/A	% de rotació per l'import de la factura del període
PEVPER02	No disponibilitat de Personal	Incompliment de l'horari de servei, la no disponibilitat de servei o la no presència en el lloc de treball del personal en qualsevol moment del període contractat.	Hores d'incompliment de servei [h] Càlcul = Total d'hores de falta de presència d'un perfil durant l'horari de servei acordat amb l'Agència. Nota: Es considerarà l'arrodoniment a l'alça (nombre sencer en hores) de la suma acumulada dels períodes de no disponibilitat. (Per exemple, 35 min es considerarà com 1 hora a efectes de penalització o 2 hores i 20 minuts com 3 hores)	Mensual	N/A	Import de 2h de servei per cada hora d'indisponiblitat.
PEVPER03	Falta de substitució de perfils	Faltes de substitució de personal quan es produeix una desvinculació.	Hores amb manca de substitució [h] Càlcul = Total d'hores de falta de presència degut a una desvinculació prèvia.	Mensual	N/A	Descompte de la meitat d'hores del perfil desvinculat en el contracte del servei.
Qualitat						
PEVQUA01	Qualitat dels lliurables del servei	Grau de satisfacció de l'Agència respecte la qualitat i contingut dels lliurables generats pel servei. Entre d'altres, els aspectes més importants definits als apartats "Lliurables del servei" i "Mètriques i indicadors".	Puntuació [de 1 (menys satisfactori) a 10 (més satisfactori)] segons enquestes de satisfacció al responsable del servei de l'Agència. El contingut de les enquestes ha de ser acordat previ a la fase de prestació del servei.	Mensual	6	5% de l'import de la facturació del període

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
PEVQUA02	Qualitat la prestació del servei	Grau de satisfacció de l'Agència respecte la prestació del servei en general, valorant entre d'altres: dedicació i rendiments del perfils assignats, assoliment de fites, incidències amb el servei, compliment de procediments/fluxos definits, etc.	Puntuació [de 1 (menys satisfactori) a 10 (més satisfactori)] segons enquestes de satisfacció al responsable del servei de l'Agència. El contingut de les enquestes ha de ser acordat previ a la fase de prestació del servei.	Mensual	6	Fins a un 5% de l'import de la facturació del període
Gestió documental						
PEVDOC01	Manteniment de la informació rellevant del servei.	Nivell de revisió i manteniment dels procediments i instruccions operatives del servei. La disposició de documentació dels processos són clau per gestionar de manera efectiva les tasques del servei. Per aquest motiu, s'ha de disposar i mantenir actualitzada qualsevol documentació que permeti garantir el compliment dels processos interns del servei.	Percentatge de documents actualitzats [%]. Càlcul = (Número de documents mensuals actualitzats) / (número documents mensuals a actualitzar) * 100. On el número de documents actualitzar mensualment haurà de ser calculat en base a la quantitat del total de documents operatius del servei.	Mensual	95%	Fins a un 5% de l'import de la facturació del període
Eficiència						
PEVEFI01	Gestió eficient de les comunicacions amb els interlocutors principals	Gestionar en un temps raonable les peticions, consultes, requeriments, etc. que arribin al servei com a part de la seva funció	Temps en gestionar una resposta, requeriment o consulta mai superior a 1 jornada laboral.	Mensual	N >= 3	5% de la facturació del període.
PEVEFI02	Nivell d'avenç dels plans d'acció, evolució, millora i assoliment de fites.	Grau d'execució i avenç dels plans d'acció, evolució, millora i assoliment de fites, basats en les tasques de seguiment i gestió del servei	Estat d'evolució segons fites i tasques planificades prèviament. En cas de no fer-se efectiva cap mena d'evolució, caldrà motivar-ne la justificació per dependència de tercers.	Mensual	70%	5% de la facturació del període.
PEVEFI03	Manca d'escalat de riscos dels projectes i iniciatives	Control dels riscos derivats de la manca de compliment de fites, terminis i altres en l'execució de projectes o iniciatives	Número de casos en els que no s'ha reportat un risc en els temps suficient (a criteri dels responsables interns de servei) per al seu	Mensual	N >= 2	5% de la facturació del període.

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
			coneixement i correcta gestió.			
PEVEFI04	Compromís amb les dates d'entrega	Incompliment de les dates acordades d'entrega dels diferents lliurables (informes, mètriques, indicadors, etc.) o fites definides.	Nombre de lliurables-productes-fites a entregar en el mes, que no han sigut lliurats [N1] Nombre de lliurables-productes-fites entregats en una data posterior a l'acordada [N2], especificant el nombre de dies desviats respecte la data d'entrega establerta [d]. Nota: En cas que l'incompliment d'un termini estigui justificat per dependència de tercers caldrà aportar el raonament oportú.	Mensual	N1 >= 1 N2 >= 3	(N1 * (3% de l'import de la facturació del període)) + ((Suma de dies desviats) * (0,5% de l'import de la facturació del període))

4.2.2.3 Bloc de servei Lot 3: Arquitectura de seguretat i evolució de solucions

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
Personal						
AREPER01	Rotació de Personal	Índex de rotació del personal presencial en el servei (queden excloses d'aquest indicador les admissions i les desvinculacions per variació del nombre d'efectius del servei per possible modificació del nombre d'efectius del servei recollida en la proposta de servei)	Índex de rotació de personal [%] Càlcul = ((admissions de personal + desvinculacions de personal presencial)/2) *100) / (nombre d'efectius del servei pel període considerat)	Mensual	N/A	% de rotació per l'import de la factura del període
AREPER02	No disponibilitat de Personal	Incompliment de l'horari de servei, la no disponibilitat de servei o la no presència en el lloc de treball del personal en qualsevol moment del període contractat.	Hores d'incompliment de servei [h] Càlcul = Total d'hores de falta de presència d'un perfil durant l'horari de servei acordat amb l'Agència. Nota: Es considerarà l'arrodoniment a l'alça (nombre sencer en hores) de la suma acumulada dels períodes de no disponibilitat. (Per exemple, 35 min es considerarà com 1 hora a efectes de penalització o 2 hores i 20 minuts com 3 hores)	Mensual	N/A	Import de 2h de servei per cada hora d'indisponiblitat.
AREPER03	Falta de substitució de perfils	Faltes de substitució de personal quan es produeix una desvinculació.	Hores amb manca de substitució [h] Càlcul = Total d'hores de falta de presència degut a una desvinculació prèvia.	Mensual	N/A	Descompte de la meitat d'hores del perfil desvinculat en el contracte del servei.
Qualitat						
AREQUA01	Qualitat dels lliurables del servei	Grau de satisfacció de l'Agència respecte la qualitat i contingut dels lliurables generats pel servei. Entre d'altres, els aspectes més importants definits als apartats "Lliurables del servei" i "Mètriques i indicadors".	Puntuació [de 1 (menys satisfactori) a 10 (més satisfactori)] segons enquestes de satisfacció al responsable del servei de l'Agència. El contingut de les enquestes ha de ser acordat previ a la fase de prestació del servei.	Mensual	6	5% de l'import de la facturació del període

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
AREQUA02	Qualitat la prestació del servei	Grau de satisfacció de l'Agència respecte la prestació del servei en general, valorant entre d'altres: dedicació i rendiments del perfils assignats, assoliment de fites, incidències amb el servei, compliment de procediments/fluxos definits, etc.	Puntuació [de 1 (menys satisfactori) a 10 (més satisfactori)] segons enquestes de satisfacció al responsable del servei de l'Agència. El contingut de les enquestes ha de ser acordat previ a la fase de prestació del servei.	Mensual	6	5% de l'import de la facturació del període
Gestió documental						
AREDOC01	Manteniment de la informació rellevant del servei.	Nivell de revisió i manteniment dels procediments i instruccions operatives del servei. La disposició de documentació dels processos són clau per gestionar de manera efectiva les tasques del servei. Per aquest motiu, s'ha de disposar i mantenir actualitzada qualsevol documentació que permeti garantir el compliment dels processos interns del servei.	Percentatge de documents actualitzats [%]. Càlcul = (Número de documents mensuals actualitzats) / (número documents mensuals a actualitzar) * 100. On el número de documents actualitzar mensualment haurà de ser calculat en base a la quantitat del total de documents operatius del servei.	Mensual	95%	5% de l'import de la facturació del període
Eficiència						
AREEFI01	Gestió eficient de les comunicacions amb els interlocutors principals	Gestionar en un temps raonable les peticions, consultes, incidents, requeriments, etc. que arribin al servei com a part de la seva funció	Temps en gestionar una resposta, requeriment o consulta mai superior a 1 jornada laboral	Mensual	N >= 3	5% de la facturació del període.
AREEFI02	Nivell d'avenç de les necessitats, models, i/o assoliment de fites.	Grau d'execució i avenç de les necessitats, models i/o assoliment de fites, basats en les tasques de seguiment i gestió del servei	Estat d'evolució segons fites i tasques planificades prèviament. En cas de no fer-se efectiva cap mena d'evolució, caldrà motivar-ne la justificació per dependència de tercers.	Mensual	70%	5% de la facturació del període.
AREEFI03	Compromís amb les dates d'entrega	Incompliment de les dates acordades d'entrega dels diferents lliurables (informes, mètriques, indicadors, etc.) o fites definides.	Nombre de lliurables-productes-fites a entregar en el mes, que no han sigut lliurats [N1] Nombre de lliurables-productes-fites entregats en una data posterior a l'acordada [N2], especificant el nombre de	Mensual	N1 >= 1 N2 >= 3	(N1 * (3% de l'import de la facturació del període)) + ((Suma de dies desviats) * (0,5% de l'import de la facturació del període))

Codi	Nom	Descripció	Fórmula de càlcul	Periodicitat	Llindar	Penalització Màxima
			dies desviats respecte la data d'entrega establerta [d]. Nota: En cas que l'incompliment d'un termini estigui justificat per dependència de tercers caldrà aportar el raonament oportú.			
AREEFI 04	Pas a producció de noves funcionalitats de manera incorrecte.	Passos a producció de noves funcionalitats que no han sigut degudament provades i que generen un impacte en forma d'incidència a la resta de serveis del SOC/CERT o generen una no conformitat amb el disseny funcional.	Percentatge de passos a producció incorrectes [%]. Càlcul = (Número de passos a producció mensuals que han generat una incidència) / (Número de passos a producció mensuals) * 100.	Mensual	<5%	5% de la facturació del període

5 FASES DE LA PRESTACIO

Per cadascun dels equips proposats, els licitadors hauran de presentar a la seva oferta tècnica el pla d'actuació detallat per tal de garantir les següents fases:

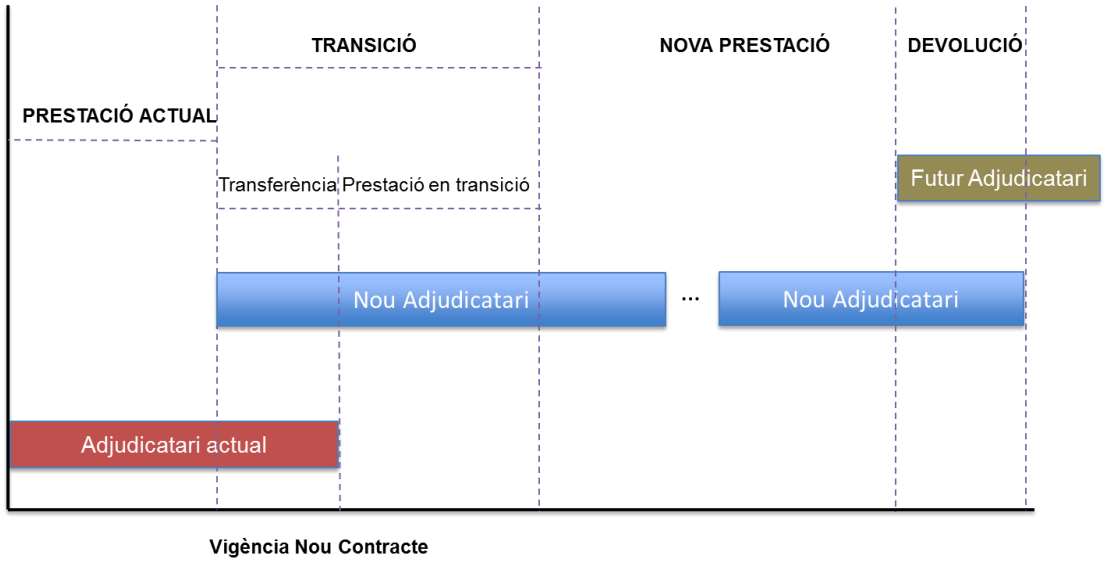

Figura 10. Fases de la prestació de servei.

5.1 Transició

És el període que va des de l'entrada en vigor del contracte fins l'estabilització dels serveis en els nivells establerts en aquest plec. La transició tindrà una durada màxima de dos mesos des de la data d'adjudicació.

Durant la transició es duran a terme les següents activitats:

- **Transferència**: El nou adjudicatari es posarà en contacte amb l'actual per dur a terme les tasques de transferència del servei, traspàs de coneixement i l'habilitació de l'operació. Durant aquesta fase l'actual adjudicatari continua prestant i facturant el servei. Aquesta fase no tindrà una durada superior a **un mes**, pel que el nou adjudicatari haurà de disposar dels efectius necessaris per començar aquest traspàs amb el suficient temps d'antelació per evitar qualsevol interrupció en el servei prestat.

  El nou adjudicatari (proveïdor entrant) haurà de combinar els seus plans amb els de l'adjudicatari actual (proveïdor sortint) i ha de ser capaç d'adquirir tot el coneixement necessari per tal de poder continuar prestant el servei tal com es dona actualment sense que hi hagi disrupcions al servei i sense que es penalitzi els possibles clients del mateix. Serà responsabilitat del proveïdor

entrant assolir aquest objectiu per a l'inici de la prestació en la data prevista en el contracte.

L'actual adjudicatari té el compromís de fer efectiu el traspàs del coneixement en les millors condicions.

- **Prestació en transició**: El nou adjudicatari comença a prestar el servei amb els seus propis mitjans. Durant aquesta etapa, el nou adjudicatari serà l'únic responsable de la prestació del servei i es comença a mesurar els indicadors de la prestació del servei, tot i que els ANS no estaran vigents i per tant no es computen penalitzacions per incompliment dels nivells de servei, exceptuant els derivats de la indisponiblitat del servei.

  Aquesta fase podrà ser modificada en funció al resultat de l'anàlisi a lliurar al final de la transferència i el pla d'acció que s'estableixi i no podrà tenir una durada superior a **un mes.**

  Si no s'iniciés la transició del servei per causes imputables a l'adjudicatari, el servei no podrà ser facturat i l'adjudicatari serà penalitzat amb l'import del servei no prestat.

En cap cas, l'Agència satisfarà cap import ni al proveïdor sortint ni al proveïdor entrant vinculat a la tasca de transició. Ambdós proveïdors només podran facturar els serveis operatius prestats respectivament a l'Agència respecte els quals, progressivament durant la transició, en cesi en la prestació el sortint i n'assumeixi la prestació l'entrant.

5.2 Nova Prestació

Es considera la fase normal de la prestació del servei. Comença quan els processos de transició hagin acabat fins un mes abans que finalitzi la prestació del servei.

Durant aquesta fase, estan vigents els plans de millora continua dels serveis i els projectes de transformació i industrialització dels serveis, liderats pel servei d'Evolució i Transformació; per aquesta raó els ANS s'han de revisar cada mes, per tal d'adaptar-los a l'evolució en la prestació dels serveis i a les variacions en el catàleg de servei i necessitats dels clients i l'Agència.

5.3 Devolució

Fase que s'emmarca al final de la prestació, un cop s'hagi comunicat la cancel·lació del contracte, i que comença **un mes** abans de l'extinció d'aquest. Durant aquest mes hi haurà coexistència amb un nou adjudicatari fins que es transfereixen els serveis a aquest. Els serveis seguiran estan subjectes a contraprestació econòmica i penalització segons els ANS.

L'adjudicatari haurà de procurar la metodologia, eines i recursos necessaris per tal de traspassar adequadament el servei a altres possibles futurs adjudicataris.

Tot el material desenvolupat, incloent desenvolupaments en Sistemes de Informació, és propietat de l'Agència i romandrà, amb tota la seva documentació, en l'Agència un cop acabada la prestació del servei.

Els mitjans tècnics que el proveïdor sortint hagi proporcionat per tal de desenvolupar la seva tasca hauran de ser degudament esborrats i tota la informació traspassada a qui l'Agència designi.

La devolució de les eines es regirà segons l'estipulat a l'apartat corresponent d'aquest plec i en les condicions acordades amb l'adjudicatari.

Juan González de Benito

Responsable Línia de Servei d'Intel·ligència i resposta activa – Catalonia Cert

6 ANNEX I – LLISTAT D'EINES

En cas que el licitador desitgi conèixer el llistat de les eines que l'Agència utilitza en l'actualitat, incloent les lligades al lloc de treball i a la estructura i continguts de les maquetes emprades pel lloc de treball, haurà d'enviar la seva sol·licitud a l'adreça de correu electrònic facilitada per a resoldre consultes sobre la present licitació (contractacio@ciberseguretat.cat).

L'Agència enviarà al licitador un acord de confidencialitat que aquest haurà d'acceptar i retornar signat. Una vegada formalitzat aquest acord de confidencialitat l'Agència enviarà al licitador el llistat d'eines.

7 ANNEX III – MARC NORMATIU

A títol informatiu, es llisten alguns dels estàndards vigents de compliment obligatori dins l'àmbit de la Generalitat de Catalunya:

- GUIT007-C - Protecció entorns Linux
- GUIT061-C - Protecció entorns Windows Server 2012
- GUIT063-C - Protecció entorns SQL Server 2012
- GUIT064-C - Protecció entorns Microsoft SharePoint 2013
- GUIT073-C - Protecció entorns Windows 7 i 8
- GUIT074-C - Protecció entorns MySQL 5x
- NOR0018-C - Norma de mesures de seguretat en la construcció de sistemes informació
- GUIT019-C - Guia de contrasenyes
- GUIT020-C - Gestió de comptes administració de sistemes
- GUIT044-C - Guia eliminació segura informació en la reutilització o destrucció de suports i sistemes
- PRC0001- C - Procediment de notificació d'incidents de seguretat
- GUIT023-C - Guia de seguretat física de CPDs i sales tècniques
- GUIT040-C - Guia de còpies de seguretat
- GUIT050-C - Guia de gestió de la continuïtat del negoci

- GUIT065-C - Trasllat de CPDs i migració de dades
- GUIT002-C - Guia d'administració del correu electrònic
- GUIT003-C - Guia d'administració de l'estació de treball
- GUIT004-C - Guia d'administració de xarxes WiFi
- NOR0016-C - Gestió de traces
- NOR0046-C - Navegació Web de la Generalitat de Catalunya
- FRM0004-C - Memòria del sistema de videovigilància
- FRM0008-C - Document d'acceptació d'obligacions relatives a seguretat de la informació i protecció de dades de caràcter personal
- GUIL071-C - Guia Legal Seguretat ENS Metodologia
- NOR0003-C - Contractació de Tercers
- GUIT026-C - Ús del correu electrònic
- NOR0005-C - Contrasenyes
- PRT0009-C - Model de protocol sobre l'ús de dispositius no corporatius
- Nota en relació amb l'ús de serveis disponibles a la xarxa que permeten compartició de fitxers i d'altres