Plec de prescripcions tècniques particulars que regeix la contractació basada relativa al suport pel servei d'Intel·ligència d'Amenaces de l'Agència en l'àmbit del govern i de l'administració de la Generalitat i el seu sector públic

CB25AMOP04001

ÍNDEX

1 Introducció

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

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

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

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

En el marc de l'activitat gestionada per l'Agència de Ciberseguretat, cal destacar que segons recull la memòria de l'Agència de Ciberseguretat de Catalunya de 2024, presentada al Govern, l'entitat ha tingut un paper rellevant en les tasques de protecció, prevenció i resiliència davant de ciberamenaces a l'Administració pública catalana durant el 2024, tant pel que fa a la Generalitat com la resta d'àmbits gestionats per l'Agència. En aquest sentit, l'Agència gestiona més de 2.200 sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants. Aquest perímetre protegit provoca un alt nivell d'activitat de gestió. Més concretament, s'han identificat més de 6.900 milions d'atacs dirigits contra els sistemes d'informació i les persones dels àmbits gestionats per l'Agència, en contraposició als 5.000 milions d'atacs del 2023. Pel que fa als incidents de seguretat, l'Agència en va gestionar prop de 3.372 durant el 2024, un augment del 26,29 % respecte als 2.665 incidents del 2023.

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

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

Avui en dia l'Agència té les següents funcions:

- **Gerència** s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació i la gestió de personal.
- **Operacions** du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció i resposta de seguretat en la seva vessant més operativa (coneguda com SOC/CERT).
- **Desenvolupament d'Estratègia d'Àmbits** (DEA) té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes i iniciatives de seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- **Producte i Centres de Competència i Innovació (DIP)** s'ocupa, per una banda, d'identificar les necessitats i proposar noves idees i estratègies per a l'elaboració de nous productes generats per l'Agència o millora dels existents, i coordina l'execució del cicle de vida dels productes, des de la seva concepció fins a la seva retirada, incloent el disseny, desenvolupament, desplegament i control de qualitat. Per una altra banda, coordina, cohesiona i capacita l'ecosistema de la Ciberseguretat de Catalunya, recolzant el coneixement, sensibilització i conscienciació com a palanca de la transformació i creixement del sector.
- **Certificacions** en matèria de Ciberseguretat per desplegar totes les eines i processos vinculats al procés de certificació en ciberseguretat de les entitats, garantint sempre la independència necessària per la correcta execució d'aquests processos.

2 Descripció dels serveis objecte de la contractació basada

2.1 Context dels serveis objecte de la licitació

El servei objecte de licitació en aquest plec està contextualitzat en l'expedient AM.02.2024 que regeix l'Acord Marc de serveis de suport a les funcions de Ciberseguretat pròpies del Centre d'Operacions de Seguretat de l'Agència de Ciberseguretat de Catalunya.

Concretament s'emmarca en el "Lot 4: Intel·ligència d'Amenaces".

Dins d'aquest lot s'inclouen, tal i com indica el Plec de Clàusules Tècniques de l'Acord Marc de referència, el suport en les tasques d'identificació, enteniment i contextualització de les ciberamenaces més rellevants, per poder donar una resposta adequada i reduir, de manera efectiva i eficient, l'afectació d'aquestes als diferents àmbits d'actuació de l'Agència.

En general, i a mode resum, l'Agència busca resoldre amb la present licitació les següents capacitats:

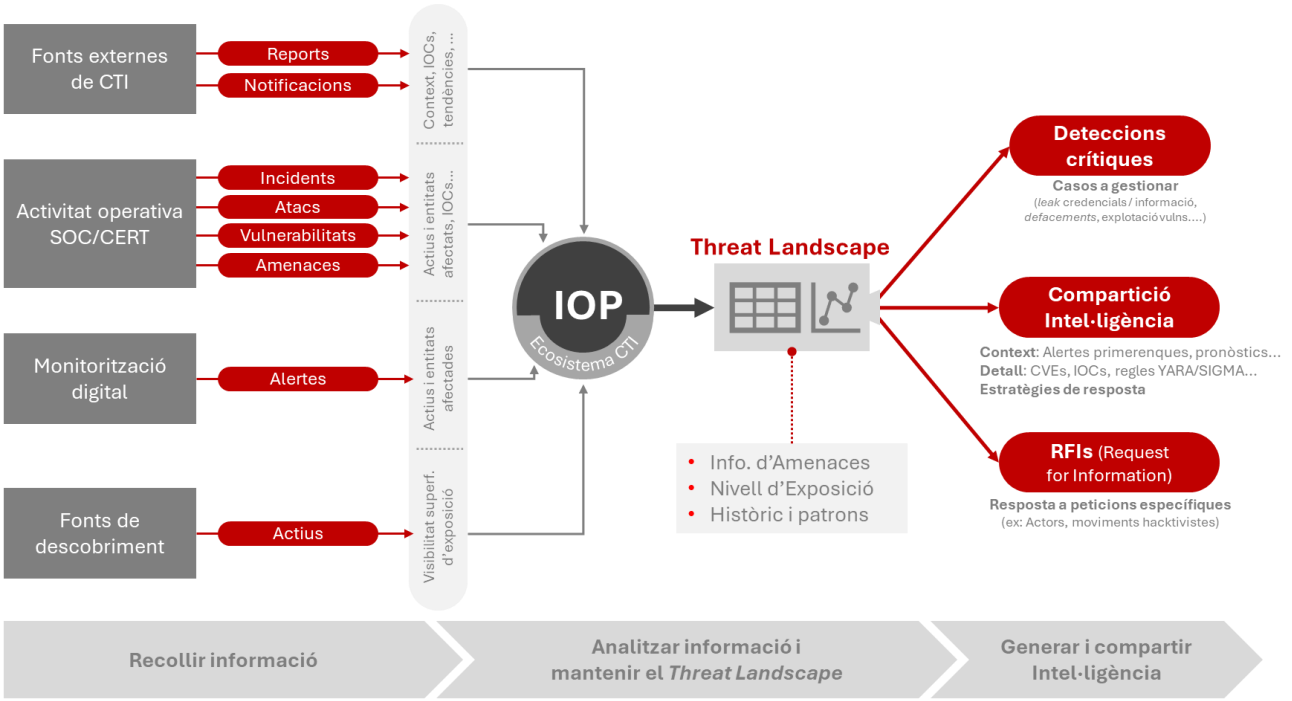
- Identificació i contextualització de les principals ciberamenaces que afecten a l'àmbit d'actuació de l'Agència, des de diferents perspectives i nivells d'abstracció.
- Suport per l'actuació eficaç i eficient envers les principals ciberamenaces, en qualsevol dels possibles àmbits d'actuació (detecció, prevenció, protecció i resposta).
- Model de gestió i govern per als serveis finalistes dins de la funció d'Intel·ligència d'Amenaces
- Evolució i millora del servei durant la vigència de la licitació.
- Retenció del coneixement, així com independització de les persones.

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

2.2 Serveis recurrents d'Intel·ligència d'Amenaces

2.2.1 Objecte i abast dels serveis

L'objecte de la present licitació és la contractació de les tasques de suport a la gestió i operativa de la funció d'Intel·ligència d'Amenaces de l'Agència en l'àmbit del Govern i de l'Administració de la Generalitat i el seu sector públic, on aquesta funció s'encarrega de manera simplificada dels aspectes identificats a continuació (també resumit en la següent figura):



Model funcional a alt nivell de la funció d'Intel·ligència d'Amenaces

- **Recollir informació útil per** permetre la **identificació i contextualització de ciberamenaces o possibles incidents** aplicables als àmbits d'actuació de l'Agència i el seu sector públic. Aquí s'inclou, entre d'altres, la configuració d'eines específiques de CTI, establiment de processos pel tractament de tota la informació d'intel·ligència rebuda, ja sigui generada per les fonts internes de l'Agència, notificacions de fonts externes, o procedent de la resta d'activitat generada per altres equips del SOC/CERT.
- **Analitzar tota la informació recollida d'intel·ligència i mantenir l'escenari de ciberamenaces** (anomenat internament com a 'Threat Landscape'), per assegurar que l'Agència disposa de tot el coneixement necessari per entendre el comportament de cada amenaça, estimar l'exposició a aquestes dels diferents actius dins de l'àmbit d'actuació de ll'Agència, i proposar mesures per la seva prevenció. Aquí s'inclou, entre d'altres, l'enteniment de qualsevol amenaça, coneixement dels actors maliciosos potencialment implicats i els seus 'modus operandi', històric d'activitat al voltant de cada amenaça al territori català i extracció de conclusions en base a tot aquest context previ.
- **Generar i compartir qualsevol fet rellevant al voltant de les ciberamenaces**, què permeti als principals àmbits afectats conèixer les amenaces que els hi apliquen i prendre decisions amb el context adquirit. Aquí s'inclou, entre d'altres, la generació d'avisos i alertes a mode preventiu (tant a nivell intern de l'Agència com extern), compartició d'indicadors de compromís contrastats i de qualitat (IOCs), compartició d'altra informació tècnica associada a la ciberamenaça com ara TTPs, suport davant incidents o qualsevol altra investigació o petició

especial per generar context d'amenaces, així com proposta de recomanacions i estratègies de resposta per mitigar possibles impactes de les ciberamenaces identificades. Addicionalment, inclou la compartició d'intel·ligència i context operatiu amb altres CERTs i entitats anàlogues.

Per assolir l'objecte descrit anteriorment, s'identifiquen, entre d'altres, els següents serveis finalistes:

- **Identificació i seguiment de ciberamenaces.**
- **Govern d'estratègies de resposta**.
- **Assegurament i evolució de l'ecosistema CTI**

Aquests serveis tindran associades un conjunt de funcions transversals, l'objecte de les quals es descriu més endavant, i sempre vetllant per l'excel·lència operativa en termes d'eficiència i eficàcia, tant tècnica com econòmica.

En el servei de suport a la Intel·ligència d'Amenaces es requereix que l'adjudicatari doti els equips humans amb les capacitats tècniques, eines[1], habilitats i estructures organitzatives per donar suport a l'Agència en la prestació de serveis què permetin proporcionar el coneixement i els plans d'actuació necessaris per a reduir de manera efectiva i eficient l'afectació de ciberamenaces als àmbits d'actuació de l'Agència, mitjançant les metodologies, els models de treball i les activitats de relació i coordinació que es requereixin.

2.3 Serveis no recurrents d'Intel·ligència d'amenaces

En relació amb els serveis descrits anteriorment, l'Agència estableix la possibilitat de dur a terme projectes o prestacions de serveis de la mateixa naturalesa de caràcter excepcional, la volumetria dels quals no es pot preveure ni concretar en el moment d'elaborar aquest plec, en altres àmbits diferents de l'inicialment previst (però que puguin requerir més endavant també tasques de suport a les funcions de suport a la gestió i operativa de la funció d'Intel·ligència d'Amenaces).

Aquesta prestació no recurrent es durà a terme a criteri de l'Agència en funció de les necessitats en cada cas. Aquestes prestacions dependran de que, si s'escau, es rebi la petició per a dur a terme la prestació de serveis, que es disposi de la partida econòmica necessària per a dur a terme l'execució d'aquests projectes i de que el licitador ofereixi una solució competitiva en el moment en que se sol·liciti la seva execució. Serà l'Agència qui, en el seu cas, sol·licitarà durant l'execució del contracte al licitador valoració d'esforç per a dur a terme aquestes tasques no contemplades als servei principal o recurrent (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 del projecte al contractista. En cap cas serà obligatori que l'Agència encomani l'execució dels serveis no recurrents al contractista quedant a discreció de l'Agència aquesta decisió segons criteris motivats.

L'execució dels serveis inclosos en aquesta categoria se subjectarà, en el seu cas, a la proposta econòmica que el licitador formuli per als serveis recurrents d'aquesta licitació (ja que són de la mateixa naturalesa). No serà necessari doncs que el licitador proposi una solució especifica per aquests serveis no recurrents sinó que es prendrà com a referència la descripció i oferta de serveis feta per als serveis recurrents.

[1] Queden excloses les eines pròpies de l'Agència que formen part de l'ecosistema CTI i que el servei licitat haurà de fer servir en la seva operativa recurrent (veure apartat "2.4.3. Assegurament i evolució de l'ecosistema CTI", on es llisten les diferents eines i finalitats cobertes per cadascuna d'elles).

Com a exemples de possibles serveis que es poden sol·licitar serien aquells inclosos en el desplegament dels serveis actuals de l'Agència a nous àmbits de treball, com serien els següents:

- Centres hospitalaris.
- Centres sociosanitaris i de salut mental.
- Universitats.
- Entitats del sector públic de la Generalitat de Catalunya.

A efectes de volumetries, s'estima que la distribució d'esforç per àmbit oscil·laria al voltant d'un perfil expert d'amenaces dedicat per cada àmbit, el qual s'encarregaria d'identificar i donar visibilitat de les tendències d'amenaces que afecten específicament a l'àmbit en qüestió, així com fer seguiment actiu d'aquestes amenaces i els actors més rellevants involucrats, contribuint al càlcul del grau d'exposició del conjunt d'actius o entitats a aquestes amenaces. Tanmateix, fins que no es tingui la certesa de la necessitat d'incorporar les tasques pròpies d'aquesta licitació als àmbits, no es podrà concretar les volumetries exactes.

2.4 Característiques del servei

De tot el que s'ha exposat prèviament es pot observar com, a l'hora de presentar les seves ofertes, els licitadors han de tenir en compte els elements essencials identificats en els següents apartats.

2.4.1 Identificació i seguiment d'amenaces

i. Objecte i descripció

L'objecte d'aquest servei és identificar, analitzar i fer seguiment de les ciberamenaces més rellevants aplicables als entorns i àmbits a l'abast del basat, a partir de diferents fonts d'informació.

ii. Objectius del servei

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

- Disposar de capacitat de detecció proactiva d'esdeveniments rellevants per tots els àmbits d'actuació amb un rati d'efectivitat no inferior al 90%.
- Aconseguir que el CATALONIA-CERT es converteixi en principal referent de ciberseguretat dins del territori, en materia d'informació de context de les principals ciberamenaces que afectin als diferents àmbits als que l'Agència presta algun servei.
- Aconseguir que la ciberamenaça sigui l'element vehicular de tota l'activitat operativa del SOC/CERT, assegurant que com a mínim el 90% dels casos gestionats estiguin associats a una amenaça, reforçant així el concepte d'una operació "Threat Centric".

iii. Activitats i funcionalitats

El servei contempla la gestió complerta de les principals ciberamenaces, des de la seva detecció inicial, fins el seu seguiment, compartició d'intel·ligència relacionada i proposta d'accions per reduir-ne la seva exposició. Les activitats que s'esperen del servei són:

- **Monitorització i processament dels resultats de les diferents fonts d'intel·ligència** (Eines CTI de l'Agència o solucions pròpies del licitador, *feeds* externs, notificacions de

tercers, casos gestionats SOC/CERT...) per identificar i notificar qualsevol esdeveniment rellevant de manera fiable, des del punt de vista de la prevenció i la resposta en front a amenaces, que afecti, o pugui afectar, a les entitats a les que l'Agència presta servei.

El licitador podrà proposar la tipologia d'esdeveniments rellevants a detectar per cada àmbit d'actuació, però aquests conjunts com a mínim han d'incloure aspectes com:

- La venda de credencials vàlides en fòrums cibercriminals i d'altres que permetin l'accés il·legítim a infraestructures corporatives.
- La publicació de *leaks* d'informació amb credencials o informació sensible rellevant a repositoris públics o a la 'Internet Fosca' (en endavant *Dark Web*).
- El compromís i la subsegüent alteració no autoritzada d'un lloc web corporatiu.
- La publicació en xarxes socials, fòrums especialitzats o '*Dark web*' de continguts que denotin la potencial materialització d'un incident en els àmbits d'aplicació.
- De manera general, la preparació de possibles atacs contra actius dels àmbits d'actuació.

Addicionalment, de manera opcional també es consideren rellevants casos com els següents:

- La inclusió d'infraestructura legítima en una *blacklist*.
- La publicació d'una aplicació mòbil maliciosa que suplanti una aplicació legítima.

En aquesta línia, el servei licitat ha de ser capaç de detectar esdeveniments rellevants i generar la corresponent alerta a processar dins del SOC/CERT, garantint què es gestionen de manera urgent aquelles que ho requereixin, independentment de l'hora de la seva detecció (24x7). Addicionalment, ha de disposar de la capacitat per executar cerques específiques sota demanda a totes les fonts disponibles, així com recopilar informació addicional per disposar del major context possible de les amenaces que facilitin la presa de decisions i estratègies de resposta a aquestes.

- **Manteniment del '*Threat Landscape*'**, per assegurar que la funció d'Intel·ligència d'Amenaces, a partir de la correlació, ordenació, normalització i interpretació de les dades disponibles, disposa de tot el coneixement necessari per entendre el comportament i evolució de cadascuna de les amenaces identificades. Entre els aspectes més rellevants a disposar es troben:
  - Registre i classificació per categoria i criticitat de cada amenaça.
  - Comprensió de les tàctiques, tècniques i procediments (TTP) utilitzats pels actors d'amenaces.
  - Identificació de les motivacions i el públic objectiu dels actors d'amenaces.
  - Visió de l'històric d'activitat al voltant de cada amenaça, especialment al territori català, per determinar quines amenaces estan actives i quines no.
  - Assegurament de l'associació a les amenaces del '*Threat Landscape*' de l'activitat gestionada pel SOC/CERT.
  - Determinació del grau d'exposició dels diferents actius dels àmbits responsabilitat de l'Agència a les amenaces del '*Threat Landscape'*.
  - Extracció de conclusions en base a l'anàlisi de tot aquest context previ.

- Pronòstic d'evolució de l'escenari general i per àmbit, basat en l'anàlisi de tot el context disponible i previsió del canvi de comportament de les amenaces existents i les emergents.

El servei de suport licitat haurà de definir, mantenir i evolucionar els processos i models necessaris que permetran a l'Agència de Ciberseguretat de Catalunya identificar de manera permanent les amenaces rellevants aplicables als seus àmbits d'actuació i coordinar la valoració (de manera puntual o recurrent) del grau d'exposició a l'amenaça per la major part d'aquests àmbits d'actuació.

- **Compartició de context d'intel·ligència**, incloent qualsevol informació rellevant per entendre les amenaces del "Threat Landscape" des de diferents perspectives i nivells d'abstracció, depenent del seu públic objectiu, on poden trobar-se altres equips del SOC/CERT, altres àrees de l'Agència o inclòs tercers externs a l'Agència com altres CERTs o el propi àmbit d'actuació de l'Agència. Entre els aspectes més rellevants a disposar es troben, entre d'altres:
  - Suport i aportació de context d'amenaces a altres equips de l'Agència, durant qualsevol investigació que ho requereixi, incloent atacs, incidents, gestió de vulnerabilitats, o peticions d'informació específiques (RFIs).
  - Suport en l'orquestració i coordinació del SOC/CERT per assegurar alineament del focus de treball envers amenaces.
  - Suport en la definició de proves per a auditors tècnics (pentesters).
  - Suport als equips de resposta de ciberincidents en el procés de preparació davant les ciberamenaces.
  - Suport a altres equips del SOC/CERT en tasques de disseny i implementació dels seus productes, per incorporar coneixement actualitzat sobre el comportament de les ciberamenaces dins d'un model netament "Threat Centric". Per exemple, amb els equips d'Arquitectura, per dissenyar perímetres de ciberseguretat que es despleguin a les entitats de l'àmbit d'actuació de l'Agència.
  - Generació i enviament d'informes, notificacions i altres productes estàtics.
  - Proposta d'accions de prevenció adients per cada ciberamenaça i identificar les contramesures òptimes en cada cas, proveint un argument sòlid per motivar la execució de les tasques associades.
  - Compartició d'intel·ligència tècnica per millorar les capacitats de detecció i protecció contra amenaces. Per exemple: Indicadors de Compromís (IOCs) o modelatge d'actors d'amenaces (tècniques i eines utilitzades per aquests, motivació, context d'esdeveniments passats rellevants al seu voltant, etc.).

2.4.2 Govern d'estratègies de resposta

i. Objecte i descripció

L'objecte d'aquest servei és desenvolupar, distribuir i valorar el compliment de les estratègies de resposta, responsabilitat del SOC/CERT, dirigides a reduir de manera efectiva i eficient l'afectació d'amenaces als àmbits d'actuació.

ii. Objectius del servei

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

- Desenvolupar les estratègies de resposta adients pels principals tipus de ciberamenaça, per cadascun del àmbits d'actuació.
- Minimitzar el grau d'improvització dels equips operatius del SOC/CERT davant de les ciberamenaces més rellevants i incidents relacionats.

iii. Activitats i funcionalitats

Les activitats i funcions que s'esperen del servei dins del Govern d'estratègies de resposta són:

- Disseny de les estratègies de resposta adients per afrontar les principals ciberamenaces aplicables als àmbits d'actuació de l'Agència.
- Coordinació del desplegament pràctic de les estratègies dins del SOC/CERT de l'Agència.
- Seguiment i revisió periòdica de l'adequació de les estratègies definides per validar la seva aplicabilitat i correcta adequació, així com la seva actualització en cas de considerar-se necessari.

El servei licitat serà el responsable de governar i desenvolupar la col·lecció de plans operatius de resposta disponibles dins del SOC/CERT. Aquest conjunt d'estratègies es defineix de manera anticipada abans de que es produeixi una situació de crisi, per tal de garantir que en tot moment es disposa d'un pla d'actuació que permeti evitar la improvisació una vegada iniciada la gestió del cas i que, conseqüentment, asseguri una resposta efectiva i eficient enfront la ciberamenaça.

2.4.3 Assegurament i evolució de l'ecosistema CTI

i. Objecte i descripció

L'objecte del servei és l'administració, configuració, operació i evolució d'aquelles solucions tecnològiques d'intel·ligència d'amenaces emprades pel servei per recollir, tractar i compartir tota la informació relacionada amb les ciberamenaces.

ii. Objectius del servei

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

- Disposar de les eines, fonts d'intel·ligència i configuracions necessàries per poder identificar qualsevol amenaça rellevant per als àmbits d'actuació de l'Agència.
- Habilitar la capacitat analítica adient per extreure de múltiples fonts d'informació, les conclusions i context oportú per gestionar les principals amenaces que afectin als àmbits d'actuació de l'Agència.
- Disposar de la infraestructura requerida per habilitar dins del SOC/CERT un ecosistema d'intercanvi d'intel·ligència de ciberamenaces.
- Habilitar els mecanismes automàtics que permetin escalar de manera urgent (per exemple activació de guàrdia) les deteccions crítiques que requereixin la potencial movilització prioritària dels equips del SOC/CERT.

iii. Activitats i funcionalitats

Les activitats i funcions que s'esperen del servei dins del "Assegurament i evolució de l'ecosistema CTI" són:

- Implementació i configuració de les solucions CTI pròpies del licitador per detectar ciberamenaces segons els criteris acordats.
- Identificació i proposta de noves eines i solucions de seguretat a integrar com a fonts d'informació d'intel·ligència.
- Integració de les noves solucions CTI que pugui aportar el licitador amb l'ecosistema actual de CTI de l'Agència per assegurar la correcta agregació d'informació a la plataforma centralitzadora d'intel·ligència de l'Agència.
- Consolidació i neteja de tota la Intel·ligència Tècnica rebuda des de totes les fonts accessibles per l'Agència de Ciberseguretat, que pugui ser consumida entre d'altres pel propi SOC/CERT.
- Cerca retrospectiva i automatizada d'activitat maliciosa a l'àmbit a partir d'indicadors reportats des de fonts externes.
- Manteniment i proposta de millores en la configuració de les eines pròpies del ecosistema de CTI de l'Agència, per millorar la capacitat de detecció d'amenaces.
- Manteniment i implementació de millores per assegurar l'accionabilitat de tota la informació d'intel·ligència (per exemple: quadres de comandament, repositoris dedicats, interacció entre processos, etc.)
- Manteniment dels canals de compartició d'Intel·ligència.

El següent és un llistat de les tecnologies més rellevants que composen l'ecosistema CTI actual:

- MISP, per la recollida i compartició d'IOCs (propietat de l'Agència).
- OMNI, com a plataforma agregadora d'Intel·ligència d'Amenaces, desenvolupada internament i basada en Elastic Stack (propietat de l'Agència).
- OpenCTI, com a plataforma de manteniment de context de ciberamenaces (propietat de l'Agència).
- KELA, Recorded Future i Axur, com a plataformes CTI (proporcionades per l'actual prestador de servei).
- BOX, per la compartició de fitxers estàtics i compartició d'evidències (propietat de l'Agència).
- XSOAR, com a mecanisme d'automatització de processos i interacció amb altres solucions de l'Agència (propietat de l'Agència).
- OTRS, com a eina de gestió de tiquets i interacció amb altres serveis del SOC/CERT (propietat de l'Agència).

El licitador haurà de presentar en la seva oferta les solucions que disposa i funcionalitats cobertes per aquestes per assegurar el compliment dels requeriments funcionals identificats prèviament.

2.4.4 Industrialització del servei

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

En un entorn tant gran com l'àmbit que gestiona l'Agència de Ciberseguretat de Catalunya, requereix un alt nivell d'industrialització, automatització i normalització de processos. Aquesta industrialització pot ser aplicable a diferents processos, tant per la ingesta d'informació d'intel·ligència, com l'automatització del seu tractament i anàlisi, com per l'elaboració i enviament de lliurables, la compartició d'informació d'intel·ligència i altres processos.

Per la maduració i la industrialització dels serveis, qualsevol servei, procés o tasca 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.

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

- Processos que consumeixin grans esforços de recursos.
- Eines amb baix retorn, tant d'eficiència com d'eficàcia.
- Processos monolítics i aïllats, que no puguin revertir en millores d'altres processos i serveis.
- Coneixements tancats, que no comuniquin i que impedeixen el creixement de l'organització.

El procés d'industrialització dels serveis plantejats pels licitadors haurà de ser degudament documentat, demostrant la línia d'industrialització plantejada i tenint en compte quins processos i eines poden ser requerides.

El licitador haurà de plantejar en la descripció dels serveis el model d'industrialització proposat i el seu pla de desplegament en la descripció del servei. Amb aquest enfocament es volen aconseguir els objectius d'eficiència operativa.

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

2.4.5 Lliurables del servei

El model de prestació del servei haurà de contemplar la definició, els continguts i la periodicitat dels lliurables del servei. Entre els lliurables es poden considerar productes que inclouen resums de l'activitat dels serveis periòdicament, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència.

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

Document	Descripció	Periodicitat
Pronòstic de ciberamenaces per àmbit	Notificació dels casos i evolucions més rellevants que han succeït durant el període, al voltant de les 5 principals amenaces que afecten a cada àmbit d'actuació de l'Agència.	Setmanal
Informe Top Amenaces anual	Informe complert sobre les ciberamenaces més rellevants de l'any. S'inclou informació com: volumetries d'activitat gestionada pel SOC/CERT relacionada a aquestes amenaces, informació de context sobre actors maliciosos involucrats i el seu 'modus operandi', proposta de mesures de contenció i protecció davant d'aquestes amenaces i pronòstic d'evolució de les mateixes per cadascun dels àmbits d'actuació de l'Agència	Anual
Alerta de ciberseguretat	Avís proactiu sobre qualsevol ciberamenaça rellevant, per a la que es vulgui portar a terme accions preventives en els àmbits d'actuació de l'Agència.	Puntual
Informe de ciberamenaça	Informe detallat sobre qualsevol amenaça rellevant que englobi el màxim context possible d'aquesta i inclogui l'estat i evolució de la seva exposició.	Puntual
Avaluació de l'exposició a l'amenaça	Informe sobre el nivell d'exposició d'una entitat, actiu o conjunt d'actius a les amenaces més rellevants que li siguin de aplicabilitat.	Puntual
Documents de treball per valorar el nivell d'exposició a les amenaces	Formularis de treball, a partir de plantilla de l'Agència, que donin suport a la definició de proves tècniques de diagnòstic que permetin calcular el grau d'exposició a les ciberamenaces d'una entitat o conjunt de sistemes. S'inclouria informació com: eines i TTPs associats a cada amenaça i proposta a alt nivell de mesures de mitigació.	Puntual
Informes de seguiment	Informes de seguiment periòdics de l'estat de les tasques, incloent la planificació, avenços, possibles desviacions, i riscos observats durant el transcurs de totes les activitats.	Mensual

La relació de productes de la funció d'Intel·ligència Operativa, la seva periodicitat i la seva pròpia estructura i continguts podran canviar amb el temps i durant el període d'execució dels serveis que es liciten, d'acord als requisits definits per l'Agència de Ciberseguretat. Els canvis s'acordaran entre l'adjudicatari i la pròpia Agència de Ciberseguretat, garantint no generar un impacte greu en cap de les dues parts.

El licitador ha d'incloure una proposta de productes a lliurar pel servei, definint entre d'altres la seva motivació, periodicitat i potencial públic objectiu. Paral·lelament, s'haurà de considerar la petició sota demanda d'informes concrets per part de l'Agència.

Es valorarà la capacitat del licitador per produir continguts de qualitat amb la informació rellevant disponible i la capacitat d'adequar el missatge als diferents receptors, especialment quan estigui orientat a negoci.

2.4.6 Mètriques i indicadors del servei

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

Indicador	Descripció
Activitat Gestionada	Control del nombre de peticions gestionades pel servei, incloent la seva tipologia i estat.
Amenaces identificades	Nombre d'informes i ciberamenaces identificats com a part de les tasques d'identificació d'amenaces.
Amenaces tractades	Nombre d'amenaces de totes les anteriors sobre les quals s'ha portat a terme alguna gestió d'intel·ligència
Amenaces en seguiment	Nombre d'amenaces d'especial rellevància sobre les quals es fa un seguiment especial degut a la potencial afectació als àmbits d'interès.
Alertes de seguretat	Nombre d'alertes generades mensualment, mantenint un inventari que permeti disposar de traçabilitat de quines han sigut.
Exposició a l'amenaça	Nombre d'exercicis completats d'anàlisi de la exposició a l'amenaça mensualment, mantenint un inventari que permeti disposar de traçabilitat de quines han sigut.
Pronòstic d'amenaces	Nombre de pronòstics d'amenaces lliurats mensualment.
Mencions notificades	Nombre de referències en fòrums de cibercriminals o especialitzats a actius dels àmbits d'actuació identificades i notificades per cadascun dels àmbits d'actuació, gràcies a les tasques de monitorització digital.
Credencials notificades	Nombre de credencials identificades i notificades per cadascun dels àmbits d'actuació, gràcies a les tasques de monitorització digital.
Investigacions dutes a terme	Investigacions realitzades mensualment, ja sigui per donar suport a un cas operatiu rellevant (atac o incident), com per obtenir context addicional d'alguna ciberamenaça o actor maliciós específic.
RFIs resposos	Nombre de RFIs als quals s'ha donat resposta, com a suport expert d'Intel·ligència d'amenaces a altres àrees i funcions de l'Agència.

2.4.7 Volumetries actuals

Per proporcionar al licitador una referència per al correcte dimensionament de la proposta es proporcionen algunes dades de volumetries estimades observades actualment.

Concepte	Quantitat/any
Intel·ligència d'Amenaces	
Amenaces externes gestionades	**1.200**
Pronòstic d'amenaces	**122**
Requisits Prioritzats d'Intel·ligència	**10**
Nombre d'alertes primerenques de seguretat	**38**
Esdeveniments detectats amb potencial impacte imminent crític	**60**
Comptes d'usuari únics compromesos identificats	**90.000**
Requeriments d'Informació des del SOC/CERT	**150**
Monitorització digital	
Dominis web	**1.500**
Adreces IP específiques	**1.400**
Rangs d'Adreçament IP /16	**3**
Rangs d'Adreçament IP/17	**1**
Rangs d'Adreçament IP /18	**1**
Rangs d'Adreçament IP /19	**2**
Rangs d'Adreçament IP /20	**1**
Rangs d'Adreçament IP /21	**2**
Rangs d'Adreçament IP /24	**2**

3 Condicions d'execució del servei

3.1 Horaris

El servei s'haurà de prestar d'acord amb els horaris de prestació dels serveis de l'Agència, 24x7 tots els dies de l'any. No obstant, s'haurà de garantir que els perfils 100% dedicats al servei, estiguin disponibles en horari 8x5 els dies laborables. Es considera horari de dies laborables els dies que siguin laborables al centre de treball de l'Hospitalet de Llobregat.

Excepcionalment, 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, sempre i quan es consideri justificat i s'acordi prèviament entre les parts.

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

3.2 Localització física

Inicialment, els equips prestataris dels serveis estaran ubicats físicament a les oficines de l'adjudicatari o en alguna altra que ambdues parts acordin, atenent sempre a la seguretat de la informació gestionada pel servei. Tot i això, l'Agència considera que l'adjudicatari, en coordinació amb la Direcció de l'àrea de l'Agència, podria arribar a prestar/executar fins al 100% de les tasques associades als perfils dedicats al 100% al servei, amb recursos ubicats a les instal·lacions de l'Agència de Ciberseguretat a l'Hospitalet de Llobregat.

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

3.3 Equip de treball

3.3.1 Directrius bàsiques

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

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

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.
- Capacitat de col·laboració amb altres agents implicats en la prestació de serveis dins de l'Agència, fora del propi equip que conformi el servei.
- Habilitat per identificar, analitzar i resoldre problemes.

- Capacitat de treball sota pressió.
- Coneixement de català, castellà i d'anglès, parlat i escrit.
- Ampli coneixement legal, tecnològic i de negoci de seguretat informàtica i de l'entorn de l'administració pública.
- Altres necessaris per al bon desenvolupament dels serveis.

Els licitadors hauran d'incloure en la seva proposta tècnica l'esquema d'equips de treball (descrivint-ne els perfils, dedicació, organigrama, pla de treball, etc.) per a l'execució dels serveis sol·licitats en el present plec, d'acord amb les condicions i paràmetres esmentats en els apartats d'aquest plec.

No es preveu la possibilitat de transferència del personal intern de l'Agència o dels seus clients.

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

3.3.2 Perfils

Donada l'orientació en modalitat servei, l'adjudicatari podrà conformar l'estructura de l'equip de servei segons consideri oportú, disposant de la flexibilitat necessària per implicar els recursos necessaris per mantenir en tot moment el nivell de qualitat de servei exigit. No obstant, s'identifica el requeriment indispensable de disposar de les següents figures operatives 100% dedicades al servei:

- **Analistes d'intel·ligència**: responsables d'analitzar i gestionar les alertes i deteccions provinents de les diferents fonts d'intel·ligència que pugui disposar el SOC/CERT (per exemple, *feeds* especialitzats, eines de *Threat Intelligence*, notificacions externes, investigacions pròpies o cerca manual avançada).
- **Experts en amenaces**: responsables d'identificar i donar visibilitat de les tendències d'amenaces que afecten els àmbits d'actuació del contracte basat, així com fer seguiment actiu de les amenaces i els actors més rellevants, determinant el grau d'exposició del conjunt d'actius o entitats a aquestes amenaces. Addicionalment, prestaran suport per a l'entesa de qualsevol amenaça a la resta de serveis operatius que requereixin més context per desenvolupar les seves funcions i definiran les estratègies de resposta per fer front a les principals amenaces.
- **Responsables infraestructura CTI (DevOps)**: responsables que les plataformes de l'ecosistema CTI del SOC/CERT ofereixin unes capacitats d'acord amb els requisits funcionals i tecnològics de la prestació del servei.

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

- Generació, implementació i càlcul de les mètriques i els indicadors del servei.
- Seguiment periòdic sobre l'estat i evolució del servei prestat, amb el responsable intern de la funció d'Intel·ligència d'Amenaces a l'Agència.
- Aportació d'informacions objectives i subjectives que permetin a la Direcció la presa de decisions operatives, tàctiques i estratègiques relacionades amb el contracte.

- Transparència en el procés de seguiment i facturació del servei.
- Coordinació i seguiment de les activitats dels membres que formen part del servei.
- Gestió de la capacitat del servei i la seva disponibilitat.
- Gestió de riscos operatius del servei.
- Gestió i control de la informació i processos responsabilitat del servei, com procediments i instruccions operatives.
- Generació d'informes referents a incidències de servei, actes, informes executius, informes de resultats o informes de situació, entre d'altres, assegurant sempre la qualitat tècnica i executiva dels informes.
- Suport a la resolució de conflictes i incidències operatives durant la prestació del servei.
- Detecció d'oportunitats de millora o evolució del servei i definició i coordinació d'execució d'un Pla de transformació per assegurar l'aplicabilitat d'aquestes i la seva implantació.
- Assegurament de la qualitat del servei prestat i dels lliurables generats (*Quality Assurance*).

Els requeriments mínims dels perfils professionals identificats i que poden composar l'equip són els següents:

PERFIL	REQUISITS
Analista d'intel·ligència	• Mínim 2 anys d'experiència demostrable en el món de la seguretat. • Coneixements en processament i anàlisi de múltiples fonts d'informació per a la identificació de ciberamenaces rellevants. • Coneixements de les principals amenaces a l'àmbit de la ciberintel·ligència. • Coneixements d'elements i de solucions tecnològiques de seguretat. • Coneixements analítics per abastar tot l'escenari d'una amenaça. • Coneixement de marcs de referència com MITRE ATT&CK, Diamond Model i Kill Chain. • Coneixements en la recerca d'intel·ligència mitjançant fonts de codi obert (OSINT).

Expert en amenaces	• Mínim 3 anys d'experiència demostrable en el món de la seguretat.
	• Coneixements en la investigació i l'anàlisi d'amenaces i vectors d'atac.
	• Coneixements en eines de recerca i anàlisi d'informació.
	• Participació prèvia en projectes o serveis de 'Threat Intelligence' on hagi desenvolupat com a mínim tasques de:
	  ○ Perfilament d'amenaces segons marcs de referència com MITRE ATT&CK, Diamond Model i Kill Chain
	  ○ Proposta d'accions i contramesures, com a resposta davant d'incidents i ciberamenaces.
	  ○ Elaboració d'informes executius i tècnics sobre escenari d'amenaces
	  ○ Participació en la identificació de noves fonts d'informació (xarxes socials, fòrums, estudis d'altres institucions, etc.) per a l'anàlisi de ciberamenaces, vulnerabilitats, incidents de seguretat, etc.
	• Capacitat organitzativa i resolutiva.
	• Coneixement de les 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,

PERFIL	REQUISITS
	implementacions criptogràfiques incorrectes, gestió deficient d'errors i excepcions etc.) així com les propostes de mitigació cost/efectivitat més adients.

Responsable d'infraestructura CTI (DevOps)	• Mínim 2 anys d'experiència demostrable en el món de la seguretat.
	• Participació prèvia en projectes o serveis d'integració i administració d'eines de CTI, on hagi desenvolupat com a mínim tasques de:
	  ○ Implantació i configuració de solucions d'intel·ligència d'amenaces 'open source' i de diferents fabricants de referència al mercat.
	  ○ Desenvolupament d'integracions de solucions d'intel·ligència amb altres solucions de seguretat o analítica de dades.
	• Experiència en programació i desenvolupament de programari amb Python, Java, C, C++, PHP, Bash, JavaScript, HTML, SQL.
	• Coneixements de sistemes operatius, xarxes, bases de dades, programari de control, programari de treball, programari de seguretat perimetral i monitorització.

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

3.3.3 Dimensionament i dedicació

Donada l'orientació en modalitat servei, no es requereix una definició explícita del nombre total d'hores.

No obstant això, l'estimació aproximada d'hores efectives necessàries per als perfils 100% dedicats per l'execució dels serveis demanats en aquest plec és de **4.400 hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	Hores anuals mínimes
Analista d'intel·ligència amb mínim de 2 anys d'experiència	**1.760 hores**
Expert en amenaces amb mínim de 3 anys d'experiència	**1.760 hores**
Responsables infraestructura CTI (DevOps) amb mínim de 2 anys d'experiència	**880 hores**

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

3.4 Canvi de recurs

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

3.5 Control de rotació

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

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

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

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

3.6 Eines i equipament per a la prestació de serveis

Les principals eines requerides (eina de tiqueting, gestió d'esdeveniments i alertes, sistema de registre i plataforma central agregadora d'intel·ligència d'amenaces...) per la prestació del servei seran proporcionades per l'Agència. L'adjudicatari haurà de fer servir aquestes eines, no podent extreure informació fora de l'àmbit d'actuació per la seva manipulació o explotació sense autorització prèvia de l'Agència. D'altra banda, l'adjudicatari haurà de proporcionar el conjunt de solucions necessàries per cobrir les capacitat de detecció d'amenaces indicades prèviament (veure apartat "2.4.1. Identificació i seguiment d'amenaces \ Activitats i funcionalitats").

L'Agència proveirà a les persones que prestin els serveis:

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l'Agència.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides l'Agència.
- Línies i terminals de telefonia mòbil per donar cobertura als serveis de guàrdia.
- Accés a Internet a través de la xarxa sense fils de l'edifici CTTI.

- Accés a adreces o pàgines web que siguin necessàries per al correcte desenvolupament del servei.
- Solucions de VPN i d'escriptori remot (AVD / Windows 365) per accedir als recursos i eines corporatives.
    - L'accés a les solucions corporatives (incloent AVD o Windows 365) estarà condicionat al compliment de les polítiques d'accés definides per l'Agència, mitjançant mecanismes com Azure AD Conditional Access, MFA i restriccions de sessió.
    - El maquetat i desplegament de les eines d'escriptori remot estarà gestionat i supervisat pels equips del Govern TIC i Seguretat Corporativa

L'Agència no proveirà:

- Ordinadors (ni de sobretaula ni portàtils) amb sistema operatiu.
- Solucions de Threat Intelligence (CTI)
- Telefonia fixa a les instal·lacions de l'Agència
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.
- Cap altre recurs no especificat explícitament.

En conseqüència, els adjudicataris hauran de:

- Subministrar tots elements de maquinari, sistema operatiu, programari ofimàtic i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments de l'objecte del contracte.
- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.
- Assegurar que tant el sistema operatiu com el programari ofimàtic i navegadors, compleixin amb els requeriments mínims de seguretat (solucions actualitzades i suportades pels diversos fabricants, disposar d'una solució EDR, etc.).

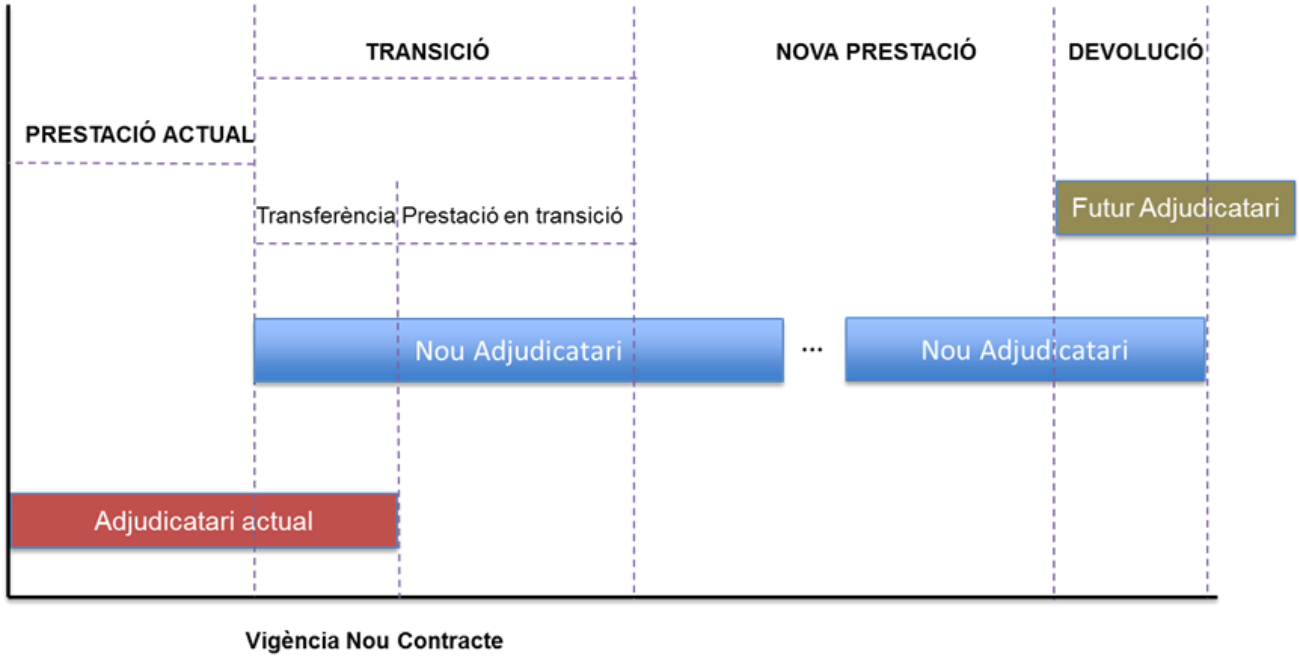
L'Agència es troba en un procés de revisió i millora contínua que pot implicar la realització de canvis importants en el referent a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei.

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

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

3.7 Fases de la prestació

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:



Fases de la prestació del servei.

3.7.1 Transició

És el període que va des de l'entrada en vigor del contracte fins a l'estabilització dels serveis en els nivells establerts en aquest plec. La transició tindrà una durada aproximada 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 adjudicatari 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 a 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 d'aquest. 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 del plec té el compromís de fer efectiu el traspàs del coneixement en les millors condicions.

A l'Agència se li haurà presentar un *checklist* dels processos, solucions i/o tecnologies conforme han estat correctament traspassades. La seguretat, com no pot ser d'una altre manera, es un eix principal, per tant tots els elements relacionats amb la seguretat hauran de tenir especial atenció amb aquest *check*.

Al final d'aquesta transició l'adjudicatari haurà de proporcionar un anàlisi de diferències (*GAP analysis*) a l'Agència entre la configuració dels serveis en el moment de la transició i la situació que s'ofereixi a la seva proposta per definir un pla d'acció per assolir poder assolir les condicions de servei exposades a la proposta. A partir d'aquest anàlisis, juntament amb l'Agència, s'establirà un abast, planificació i dedicacions per considerar l'adequació i nivells a assolir a la fase de prestació en transició.

- **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 haurà de ser d´una durada superior d'un mes.

  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.

  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 l'Agència respecte dels quals, progressivament durant la transició, en cesi en la prestació el sortint i n'assumeixi la prestació l'entrant.

3.7.2 Nova Prestació

Es considera la fase normal de la prestació del servei. Comença quan els processos de transició hagin acabat fins 1 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 per l'àrea d'Evolució i Transformació; per aquesta raó els ANS s'han de revisar com a mínim cada sis mesos, 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.

3.7.3 Devolució

Fase que s'emmarca al final de la prestació, un cop s'hagi comunicat la cancel·lació del contracte, 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.

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

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

En cap cas el licitador deixarà inservible qualsevol eina (incloent el llicenciament) que hagi pogut emprar durant el temps que a estat desenvolupant la seva funció.

Tal com s'ha descrit a la secció d'eines i equipament per a la prestació, els Enginyeria de Sistemes d'Informació 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.

3.8 Gestió del coneixement

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

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

3.9 Seguretat Corporativa

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

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

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

3.10 Control de Gestió

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

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

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

3.11 Documentació

L'Agència és el propietari de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris i el seu personal i subcontractats que destini a l'execució dels serveis. L'adjudicatari s'encarregarà de disposar de totes les autoritzacions i permisos necessaris per tal de poder donar compliment a aquesta previsió, essent responsabilitat de l'adjudicatari qualsevol pagament o reclamació relativa a aquesta manca d'autoritzacions.

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

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

3.12 Contingència

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

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

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

3.13 Metodologia, estàndards i lliurables

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

3.14 Seguretat

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

3.14.1 Deure de confidencialitat

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

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

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

3.14.2 Dades de caràcter personal

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

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

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

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

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

3.14.4 Capacitat tècnica

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

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

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

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

etc.), aquests hauran de ser compatibles amb l'arquitectura de seguretat de l'Agència i complir amb els requeriments de seguretat que estableixi el marc legal i el marc normatiu intern, sotmetre's a proves tècniques de seguretat i aplicar les correccions necessàries prèviament a la posada en producció del producte/solució/eina. Caldrà incorporar el producte/eina dins el procés de desenvolupament segur de l'Agència de Ciberseguretat des de la fase de disseny fins a la posada en producció.

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

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

3.14.6 Interconnexions

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

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

3.14.7 Verificació del compliment i auditoria

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

3.14.8 Incidents de seguretat

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

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

3.14.9 Accés a la informació

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

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

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

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

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

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

3.12. Seguiment del servei

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

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

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

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

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

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

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

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

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

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

3.13. Integració amb altres equips

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

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

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

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


ciberseguretat.gencat.cat