Plec de prescripcions tècniques particulars que regeix la contractació basada relativa operacions del centre d'operació de la ciberseguretat a l'àmbit salut

Exp. CB25AMOPL1B002

Índex

1 Introducció

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

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

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

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

En el marc de l'activitat gestionada per l'Agència de Ciberseguretat, cal destacar que aquesta gestiona més de 2.200 sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants. Aquest perímetre protegit provoca un nivell d'activitat de gestió de més de 4.424 milions de ciberatacs durant el 2022, una xifra 20 cops superiors a la del 2021.

D'aquests 4.424 milions de ciberatacs gestionats, 2.175 van esdevenir en un incident efectiu de seguretat gestionat per l'Agència de Ciberseguretat, el que representa una reducció del 22% respecte de l'any 2021.

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

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

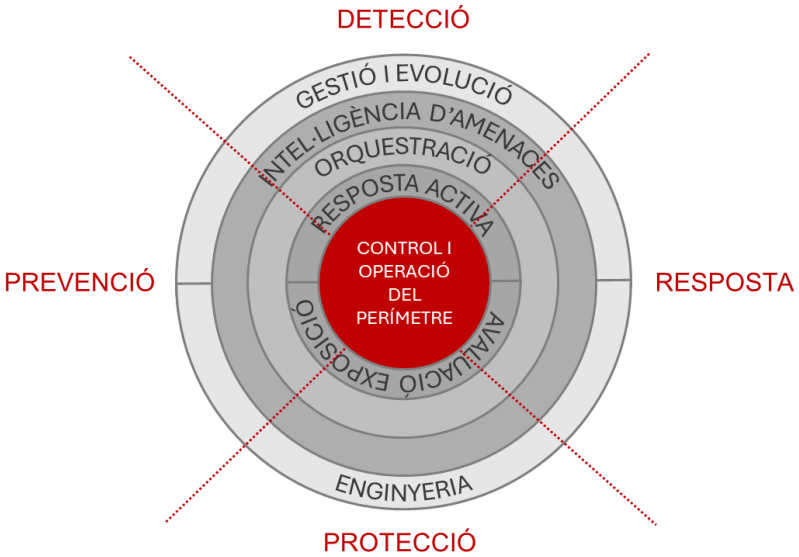
Avui en dia l'Agència té les següents funcions:

- L'Àrea de Gerència s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació i la gestió de personal.
- Operació de la Seguretat du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció, resposta i recuperació de seguretat en la seva vessant més operativa i la seguretat corporativa.
- Desenvolupament d'Estratègia d'Àmbits té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes i iniciatives de seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- Àrea de Producte s'ocupa d'identificar les necessitats i proposar noves idees i estratègies per a l'elaboració de nous productes generats per l'Agència o millora dels existents, i coordina l'execució del cicle de vida dels productes, des de la seva concepció fins a la seva retirada, incloent el disseny, desenvolupament, desplegament i control de qualitat.
- Centre de Competència i Innovació en Ciberseguretat (CCI) s'ocupa de la coordinació, cohesió i capacitat de l'ecosistema de Cibeseguretat de Catalunya, recolza el coneixement, sensibilització i conscienciació, i la innovació com a palanca de transformació i creixement del sector i fomenta la captació de forns i la internacionalització de l'entitat.
- Certificacions en matèria de Ciberseguretat per desplegar totes les eines i processos vinculats al procés de certificació en ciberseguretat de les entitats, garantint sempre la independència necessària per la correcta execució d'aquests processos.

1.2 Funcions del SOC/CERT

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

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



Estructura funcional actual del SOC/CERT

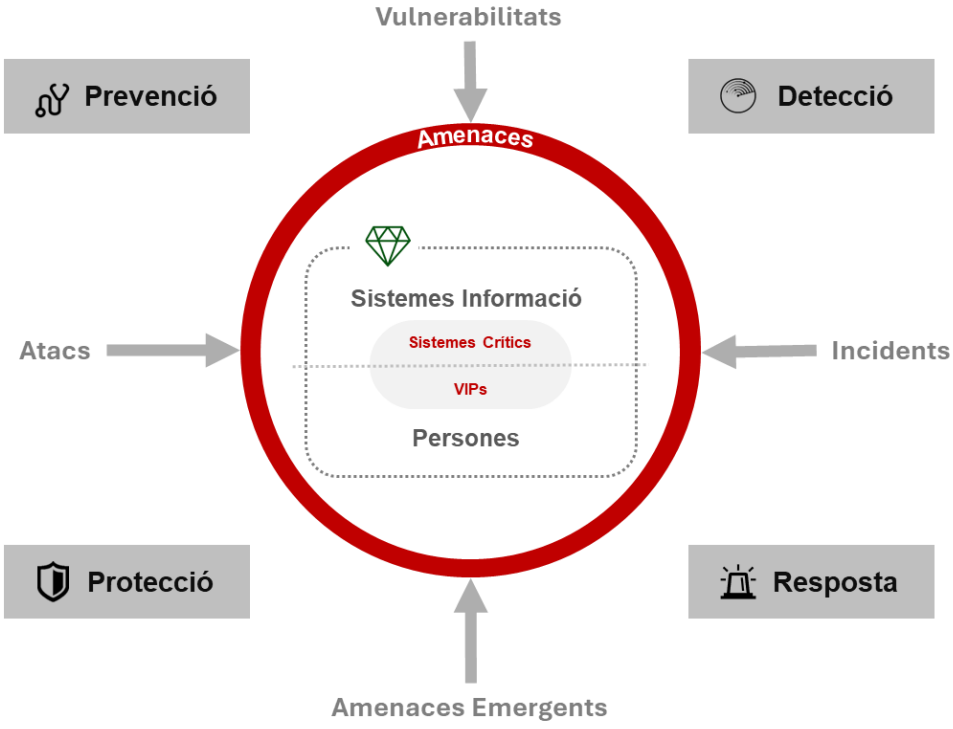
La primera funció és la de Control i Operació del Perímetre (COP), que dona resposta a la operació de perímetres dels eixos de detecció, prevenció protecció i resposta. Aquesta funció correspon a tasques relatives a la gestió del cicle de vida dels esdeveniments, vulnerabilitats, amenaces i atacs de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

La funció de "Avaluació d'Exposició" (AVX) dona suport a la resta de funcions, avaluant i validant de manera proactiva els mecanismes i controls establerts respecte als quatre eixos de detecció, prevenció, protecció i resposta, per identificar punts de millora, a més a més s'encarrega de tenir controlada l'exposició de tot l'àmbit. Els serveis objecte de la present licitació s'emmarquen precisament dins d'aquesta funció.

Tot i l'efectivitat dels controls i les tasques de prevenció desplegades, encara existeix la possibilitat de que una amenaça es materialitzi en un incident de ciberseguretat. Aleshores, la funció de Resposta Activa (RAC) s'activa de manera reactiva quan es detecta un incident de severitat elevada, per permetre reduir en temps i forma la seva afectació dins de l'àmbit i per garantir que el mateix tipus d'incident no torna a succeir en les mateixes circumstàncies. Addicionalment, aquesta mateixa funció de manera proactiva i transversal complementa a la d'AVX i realitza cerca d'amenaces 'huntings' per identificar possibles incidents i altres punts de millora.

Al voltant de les funcions més operatives del SOC/CERT es desplega l'activitat d'Orquestració Operativa, que permet garantir que tots els esforços dels diferents equips es centren en tot moment en els mateixos focus. Respecte a l'operació recurrent, l'orquestració també permet assegurar que per cada element a tractar (bé sigui una vulnerabilitat, un atac, un incident o una nova amenaça), es treballa sempre des d'un punt de vista construït sobre l'amenaça com a element central (Threat-Centric), el que permet assegurar tots els requeriments necessaris per una prevenció i una resposta efectiva i amb garanties.

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



Plantejament “Threat-Centric”

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

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

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

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

Per últim, de manera transversal, la funció de “Governança i Evolució de l’Operació” permet evolucionar el SOC/CERT, garantir la gestió eficaç dels recursos i capacitats de les diferents funcions del SOC/CERT, i posar en valor tota l’activitat operativa portada a terme pels seus equips.

1.3 El sistema sanitari

Els estudis de tendències constaten que els atacs cibernètics a centres sanitaris poden provocar greus impactes en la qualitat assistencial als pacients, poden impedir l’accés als expedients mèdics i bloquejar el funcionament de tots sistemes informàtics, i per tant, provocar retards en els procediments i proves, i hospitalitzacions més llargues.

En aquest context, l’Agència de Ciberseguretat va detectar més de mil milions d’atacs dirigits contra el sector sanitari a Catalunya durant el 2023, dels quals 308 van materialitzar-se en incidents. Alguns d’ells, com els succeïts a l’hospital Clínic o al Moises Broggi (Consorci Sanitari Integral) van suposar un greu impacte assistencial per la ciutadania, ja que van afectar de forma directa als principals hospitals i centres d’atenció primària del nucli de Barcelona.

Davant d’aquesta situació l’Agència de Ciberseguretat ha dissenyat i està desplegant un Model Integral de Ciberseguretat (en endavant, el Model), que té com a objectiu protegir els àmbits d’actuació públics més rellevants a Catalunya de les amenaces en ciberseguretat dirigides contra els seus sectors, i abordar les actuacions necessàries per a protegir-los dels ciberincidents que puguin impactar contra les diferents entitats que els conformen.

A tal efecte el Model preveu l’execució de les següents fases per al seu desplegament:

- **Diagnòstic:** identificació del grau actual d’exposició a les principals ciberamenaces que apliquen a l’àmbit.
- **Pla de seguretat:** determinació del pla de seguretat de cada entitat per tal de ser més resilient i reduir l’exposició a les amenaces més significatives, amb una orientació a assolir el compliment normatiu en l’Esquema Nacional de Seguretat i, quan correspongui, en altres normatives sectorials o específiques que siguin d’aplicació.

- **Integració operativa:** desplegament, a partir de les capacitats de protecció desplegades per les entitats, de les capacitats de prevenció, detecció i resposta, i dels processos i serveis associats a la integració amb l'Agència de Ciberseguretat de Catalunya.
- **Protecció:** activació i operació del serveis de monitorització i resposta 24x7 de l'Agència, i dels serveis i oficines necessàries per a la governança, comunicació, formació i evolució en la ciberseguretat.
- **Certificació:** procés de certificació mitjançant les auditories de la conformitat en l'Esquema Nacional de Seguretat.

Tota l'operació de la seguretat que contempla aquest Model gira al voltant del concepte "perímetre de ciberseguretat", entenent-se per perímetre el conjunt d'activitats i tecnologies desplegades i governades pel SOC/CERT, que contribueixen a la millora de la ciberseguretat dels sistemes d'informació, infraestructures transversals o de les persones.

Per a materialitzar tot l'anterior, el Servei Català de la Salut i l'Agència de Ciberseguretat de Catalunya van signar la sol·licitud d'actuació SOC-5100-25-003 en el marc del Contracte Programa de l'Agència de Ciberseguretat de l'Agència 2024-2027, el qual ha estat aprovat per Acord de Govern de 8 d'abril de 2025, en el que s'aproven les despeses amb càrrec a pressupostos d'exercicis futurs, per un import total de 27.000.000,00 euros, per al finançament de determinades actuacions de Ciberseguretat sobre el SISCAT.

L'objectiu de dita petició és la realització d'actuacions de Ciberseguretat sobre els Sistemes d'Informació de Salut, els hospitals i entitats proveïdores del SISCAT incloent les 3 línies assistencials: atenció especialitzada, sociosanitaris (intermèdia) i salut mental, i atenció primària per tal de millorar la resiliència i les capacitats de protecció, prevenció, detecció i resposta en matèria de Ciberseguretat del sistema sanitari públic de Catalunya així com avançar cap a la certificació en l'Esquema Nacional de Seguretat (ENS).

2 Descripció dels serveis objecte de la licitació

2.1 Context dels serveis objecte de la licitació.

El servei objecte de licitació en aquest plec està contextualitzat en l'expedient CB25AMOPL1B002 que regeix l'Acord Marc AM.02.2024.

Concretament s'emmarca en el Lot 1 referent a Operació de la seguretat.

Dins de dit lot s'inclouen les actuacions tal i com indica el Plec de Clàusules Tècniques de l'Acord Marc de referència serà el servei responsable **d'operar i governar les diferents fronteres de ciberseguretat definides i desplegades en els diferents àmbits** competència de l'Agència, incloent el suport a l'Agència en totes les tasques pròpies i contínues de prevenció, detecció, protecció i resposta al perímetre pel qual ha de garantir la seva seguretat, les quals son plenament assimilables a l'objecte de la present licitació.

2.2 Serveis

2.2.1 Objecte i abast dels serveis

L'objecte de la present licitació és la contractació dels serveis de suport a les operacions del centre d'operació de la Ciberseguretat de l'àmbit de Salut comprenent centres hospitalaris, sociosanitaris i d'atenció primària. Concretament, el suport en les funcions d'expertesa de seguretat, excloent així les tasques relatives a anàlisi de seguretat (N1).

Com a centre responsable de la ciberseguretat, l'Agència ha de realitzar tasques de prevenció, protecció, detecció i resposta davant de ciberatacs. Per a aquesta finalitat, el Centre d'Operació de la Seguretat (també anomenat SOC per les seves sigles en anglès) de l'Agència, disposa dels serveis de:

- **Operació de Perímetres de Seguretat de Salut (COP-SLT)**

A l'Agència, l'operació de la seguretat gira al voltant del concepte "perímetre de ciberseguretat". Entenem per perímetre el conjunt d'activitats i tecnologies desplegades i governades pel SOC, que contribueixen a la millora de la ciberseguretat dels sistemes d'informació, infraestructures transversals o de les persones.

El servei del COP-SLT es focalitza en la gestió del cicle de vida de les vulnerabilitats, esdeveniments, atacs de ciberseguretat i la gestió d'amenaces, amb l'objectiu principal de prevenir, protegir, detectar i resoldre possibles atacs a la seguretat que afectin els sistemes d'informació. Aquest equip està orientat a realitzar totes les tasques sobre els Hospitals, Centres Sanitaris o Aplicacions de la Generalitat de l'àmbit de Sanitari. L'equip és governat o orientat per l'equip de COP, però de manera independent ha de mantenir una estreta relació amb la resta de serveis per tal de mantenir una evolució i una millora continua del perímetre de seguretat, envers la identificació de vulnerabilitats, amenaces i incidents trobats en els diferents actius per assegurar que el perímetre estigui protegit fins que aquestes vulnerabilitats es resolguin.

D'aquesta manera, des del COP-SLT es realitza una tasca contínua de prevenció, detecció, protecció i resposta al perímetre pel qual ha de garantir la seguretat de totes les entitats incloses en l'àmbit sanitari.

2.2.2 Serveis no recurrents

Addicionalment als serveis recurrents descrits anteriorment, l'Agència també podria arribar a necessitar suport addicional de Control i Operació del Perímetre de Salut, principalment a les entitats prestadores de serveis sociosanitaris i salut mental. Aquests serveis es consideraran com a no recurrents.
L'Agència estableix la possibilitat de dur a terme projectes o prestacions de serveis de naturalesa anàloga als definits a l'apartat 3.2.1, el dimensionament dels quals no es pot preveure ni concretar en el moment d'elaborar aquest plec per no haver executat les fases prèvies de desplegament del model.
Aquesta prestació no recurrent es durà a terme a criteri de l'Agència en funció de les necessitats que es concretin durant el diagnòstic inicial del grau d'exposició de les amenaces i la fase de posada en servei. Aquestes prestacions dependran de que, si s'escau, es disposi de la partida econòmica necessària per a dur a terme l'execució d'aquests projectes i de que l'empresa licitadora ofereixi una solució competitiva en el moment en que se sol·liciti la seva execució.
Atenent a l'objecte de la present licitació així com a les actuacions previstes en la sol·licitud d'actuació firmada entre l'Agència de Ciberseguretat i el Servei Català de Salut, a continuació es llisten exemples de serveis o projectes que es poden sol·licitar en aquest nivell de prestació, sense ser excloents:

- Operació i gestió de Perímetres de Ciberseguretat
- Prevenció de Ciberamenaces
- Protecció enfront ciberatacs
- Identificació, anàlisi i gestió de vulnerabilitats
- Definició, implementació i manteniment de casos d'ús

2.2.3 Descripció

2.2.3.1 Operació de Perímetres de Seguretat de l'àmbit de Salut

El servei té com a objecte principal la operació i governança dels diferents perímetres de ciberseguretat definits i desplegats en les entitats de l'àmbit sanitari, els quals inclouen principalment les següents tasques:

- La gestió dels esdeveniments rebuts que esdevinguin en atacs. Això consisteix en la revisió i gestió proactiva dels esdeveniments, sigui pels dispositius de seguretat o comunicades per tercers, amb l'objectiu de, per una banda, mitigar els atacs i per altra, detectar possibles incidents de seguretat mitjançant l'anàlisi de les alertes rebudes i dels atacs identificats.

- Anàlisi d'amenaces per identificar el grau d'exposició o afectació als perímetres de l'àmbit sanitari. Aquestes amenaces poden venir identificades per altres serveis del SOC o mitjançant la revisió de diferents fonts d'informació prèviament configurades.

- La gestió del cicle de vida de les vulnerabilitats de seguretat amb la qual es permet analitzar la robustesa dels actius davant un atac. És una pràctica de seguretat orientada a la reducció preventiva de la possible explotació de vulnerabilitats dels elements que s'utilitzen en les organitzacions amb l'objectiu de reduir el nombre d'incidents de seguretat, i la seva afectació.

- Definició, implementació i manteniment de casos d'ús al SIEM de manera que permeti generar les alertes prioritàries en funció de les principals amenaces i que permeti tenir un registre i seguiment del volum, classificació i efectivitat entre d'altres punt rellevants. De manera excepcional, per millorar l'eficiència de les operacions a nivell del SOC, aquests casos d'ús aplicaran a les entitats de l'àmbit sanitari però també han de poder-se aplicar a altres entitats fora d'aquest abast.

Per tant, l'execució del servei requereix una revisió contínua dels esdeveniments i notificacions que es reben, per poder identificar aquells objectes de tractament. Entre les diferents tasques que es duen a terme en la gestió d'alertes, anàlisi d'amenaces i gestió de vulnerabilitats, hi ha:

- **Identificació d'atacs**: es tracten i es revisen els esdeveniments rebuts, realitzant un monitoratge constant, alertes generades a partir de les eines o comunicats per tercers per a la identificació d'atacs.
- **Definició, implementació i manteniment de casos d'ús al SIEM**
- **Anàlisi de context dels atacs**: per establir possibles relacions amb altres atacs identificats, que permetin identificar patrons d'atac.
- **Revisions periòdiques de patrons d'atac**: quan un esdeveniment es dona de forma repetida es genera un seguiment per revisar si es tracta d'un patró d'atac i si és necessari gestionar tant la modificació de firmes digitals, com regles per a la prevenció d'atacs, en tot moment tenint en compte la millora continua en la protecció del perímetre.
- **Gestió d'avisos i alertes de tercers:** s'analitzen els avisos i alertes procedents de tercers, o del sistemes de monitoratge de la Generalitat de Catalunya, i incorpora la informació per tal de procedir a definir millores en del perímetre de seguretat de l'Agència.
- **Contenció de vulnerabilitats conegudes**: cal realitzar la comprovació de les mesures de contenció temporals aplicades per tal de prevenir l'explotació de les vulnerabilitats detectades, assegurant-se la protecció del perímetre.

- **Addició i extracció de Indicadors de Compromís (IOC) als sistemes de seguretat del perímetre**.
- **Accions de bloqueig enfront atacs**: mitjançant procediments d'operació on s'identifiquin les tasques de contenció.
- **Identificació d'Incidents**: reportant a l'equip de resposta a incidents les evidencies necessàries que permetin gestionar l'incident.
- **Identificació i anàlisi de vulnerabilitats**
- **Gestió del cicle de vida de les vulnerabilitats**
- **Anàlisi d'amenaces,** revisió d'informació disponible a fonts o eines prèviament configurades i càlcul del grau d'exposició o afectació.
- **Participació en la gestió de problemes de seguretat**
- **Participació en comitès de crisi.**
- **Definició, implmenetació i manteniment de casos d'ús al SIEM**
- Qualsevol altra tasca anàloga.

Per altra banda, el servei també requereix que de forma proactiva s'apliquin noves polítiques de seguretat (identificació i protecció davant d'atacs) als diferents elements existents amb la finalitat d'optimitzar la capacitat de detecció i bloqueig d'atacs dirigits a la infraestructura.

Amb l'objectiu de dur a terme satisfactòriament aquests subserveis, el servei requerirà el desenvolupament de, com a mínim, les accions que es detallen a continuació:

2.2.3.2 Gestió de perímetres de seguretat de l'àmbit sanitari

- Definició i sol·licitud de noves regles de correlació/protecció/control sobre els actius del perímetre de seguretat com poden ser:
- Firewalls
- IDS/IPS
- Antivirus
- WAF
- SIEM
- Proxy's
- EDR
- SOAR
- Mail-protect (Antispam)

- Definició i sol·licitud per la recepció de noves alertes i sol·licitud per l'actualització (modificació/baixa) de les alertes presents.
  S'han de definir i sol·licitar noves alertes, a partir dels esdeveniments que es recol·lecten dels actius. Aquestes sol·licituds han d'arribar correctament desenvolupades, a enginyeria.
  S'han de definir les actualitzacions i baixes de les alertes que es requereixin per tal de tenir el conjunt d'alertes definides ben afinades i coordinades amb l'estat dels actius i les necessitats del SOC.

- Definició d'actuació.
  Per cada tipus d'alerta, cal definir el tipus d'actuació que ha de dur a terme l'operador que la rebi. Aquesta definició ha d'incloure les operacions que ha efectuat i la matriu d'escalat per als casos en els quals no poguí donar una resolució per si mateix.

- Execució de les mesures operatives definides per cada alerta.
  Per cada tipus d'alerta, s'han d'aplicar les mesures operatives definides prèviament, i per aquells casos en els quals les mesures a aplicar surtin d'aquesta operativa, cal sol·licitar la seva aplicació als interlocutors adequats com p. ex. enginyeria.

- Resposta a alertes i incidents lleus
  Per aquells incidents detectats, i que sigui possible gestionar-lo mitjançant protocols definits o actuacions bàsiques, es requerirà donar resposta. En cas de no poder donar resposta, requerir una investigació més profunda o resposta avançada s'escalarà al servei de resposta a incidents.

- Generació dels registres de resultats de l'actuació sobre un alerta
  Tota la informació associada a una alerta i les accions aplicades ha de quedar reflectides en un registre de resultats que ha de seguir una plantilla preestablerta. Aquest registre ha de contenir totes les dades rellevants sobre els resultats de les accions dutes a terme.

- Definició i execució de protocols d'actuació.
  Cada tipus d'alerta deurà tenir associada la definició i l'execució d'un protocol de tractament i gestió predefinida, per tal que el COP-SLT pugui tractar el major nombre d'alertes de forma autònoma.

2.2.3.3 Prevenció de ciberamenaces en l'àmbit sanitari

- Desplegament de contramesures per la prevenció de ciberamenaces
  Cal determinar e implementar les diferents contramesures necessàries per prevenir la explotació de vulnerabilitats, vectors d'atac i/o noves ciberamenaces.

- Revisió d'informes d'estat de seguretat
  Cal definir, generar i revisar els diferents informes que proporcionen les eines de seguretat per tal de detectar possibles ciberamenaces, com poden ser el informes del SIEM, plataforma antivirus, Splunk, filtrat de continguts, entre d'altres.

- Revisió d'eines i informes d'amenaces
  S'han de atendre les alertes o notificacions d'amenaces mes rellevants, i revisar el grau d'afectació o exposició, prioritzant els diferents perímetres desplegats.

- Revisió d'anomalies per a la detecció de ciberamenaces
  Per tal de determinar possibles incidents de seguretat s'han de revisar tots aquells indicadors que donin informació de la situació de la infraestructura, com poden ser:
  - Revisió de pics anormals de tràfic.
  - Deteccions de tràfic cap a dominis maliciosos (mitjançant l'ús de data feeds)
  - Revisió de tràfic anòmal en determinats segments de xarxa.
  - Agrupacions d'esdeveniments similars per detectar atacs de força bruta.
  - Detecció d'ús d'eines eminentment malicioses (metasploit, nmap, sqlmap, etc.)
  - Detecció d'ús de ports no habituals i de canals encoberts

2.2.3.4 Protecció en front ciberatacs

- Selecció d'esdeveniments sospitosos
  Definir el criteri de selecció dels esdeveniments sospitosos. Per exemple segons l'actiu implicat, l'ip d'origen/destí, el user-agent, el port, etc.

- Filtratge d'esdeveniments

  A partir dels esdeveniments seleccionats, s'han de filtrar aquells que són falsos positius. Caldrà també, treballar contínuament per eliminar el 'soroll' (atacs i esdeveniments que no tenen lògica dins del context) per a poder ser més àgils en la seva gestió.

- Categorització d'esdeveniments

  Cal definir una categorització dels esdeveniments per tal de classificar-los, i poder-los tractar de la forma més ràpida i eficient possible. Per poder definir aquesta categorització s'han de tenir en compte el tipus d'actiu implicat, la seva funcionalitat/severitat dins la infraestructura, el tipus d'esdeveniment, han de estar alineats amb la informació del Catàleg d'amenaces de l'Agència, i del catàleg de vectors d'atac de l'Agència.

- Priorització d'esdeveniments.

  Segons la categoria i el tipus d'esdeveniment, així com la informació externa a les evidències, que es pot tenir sobre els actius afectats, cal definir una prioritat de tractament de cada esdeveniment o grup d'esdeveniments.

- Resposta i resolució d'incidents amb procediment associat

  A partir dels esdeveniments seleccionats, aquells que resultin en la detecció d'un incident, i que tinguin prèviament associat un procediment d'actuació, hauran de ser gestionats fins a la seva resolució.

- Definició de la prioritat d'actuació sobre cada atac tenint en compte el valor dels actius afectats.

  A partir de la categoria d'un atac, i dels actius implicats, cal definir la prioritat d'actuació sobre aquest.

- Definició del procediment d'actuació principal i dels procediments d'actuació secundaris.

  Per cada tipus d'atac, cal definir un procediment d'actuació principal a seguir, i en cas que aquest no pugui ser utilitzat o no tingui el resultat esperat, s'han de tenir definits altres procediments secundaris/alternatius que puguin mitigar l'afectació d'aquest.

- Identificació d'esdeveniments com a atacs.

  Mitjançant l'anàlisi dels esdeveniments s'ha d'identificar aquells que comporten un atac i que poden esdevenir en un incident de seguretat.
  És important tenir en compte que s'ha de notificar i alertar als proveïdors de servei o als usuaris de qualsevol activitat sospitosa d'atac.

- Generació dels registres de resultats de l'actuació sobre un atac

  Tota la informació associada a un atac i les accions aplicades han de quedar reflectides en un registre de resultats que ha de seguir una plantilla preestablerta. Aquest registre ha de contenir totes les dades rellevants sobre el tipus d'atac i els resultats de les accions dutes a terme, i si l'atac ha esdevingut en un incident.

- Execució procediments d'actuació principals i, en cas de ser necessari, dels procediments d'actuació secundaris per a cada atac.

  S'han de portar a terme els procediments definits per cada tipus d'atac. En cas que els procediments principals no tinguin els resultats de resolució o mitigació esperats, s'han d'intentar aplicar els procediments d'actuació secundaris definits prèviament. Si aquestes mesures no resolen l'atac, es considerarà que l'atac passa a ser un incident, i serà derivat a l'equip de resposta davant incidents.

- Proposta de contramesures per mitigar els atacs.

Conjuntament amb el punt anterior on s'ha identificat l'esdeveniment com un incident de seguretat, s'han de proposar les contramesures necessàries per contrarestar els efectes d'aquest. Aquestes propostes s'han de comunicar i donar suport en la implantació o bé al servei d'Enginyeria, que pertany a Mitjans tècnics, o bé als proveïdors de servei implicats.

- Escalat dels atacs que no s'han pogut autogestionar i deriven en incidents complexes.
  Conjuntament amb el punt anterior on s'ha identificat l'esdeveniment com un atac, i s'han aplicat les contramesures definides, si aquestes contramesures no resulten en la resolució/mitigació completa de l'atac, aquest es derivat al servei de resposta a incidents de seguretat.

2.2.3.5 Identificació, anàlisi i gestió de vulnerabilitats

- Realització dels escanejos automàtics amb les diverses eines d'escaneig
  S'han d'utilitzar les eines d'escaneig que disposa l'entitat, per tal de poder tenir visibilitat sobre els diferents aspectes d'un mateix actiu.

- Anàlisi i validació dels resultats.
  Cal dur a terme una anàlisi dels resultats obtinguts per tal de detectar possibles patrons o falsos positius, posteriorment aplicant les mesures de prevenció i protecció envers la vulnerabilitat identificada.

- Generació dels registres de resultats.
  Tota la informació associada a un anàlisi ha de quedar reflectida en un registre de resultats que ha de seguir una plantilla preestablerta. Aquest registre ha de contenir totes les dades rellevants que puguin posar de manifest l'estat de l'actiu analitzat.

- Actuacions de suport a la mitigació de vulnerabilitats.
  Periòdicament s'haurà de fer un anàlisi de les vulnerabilitats trobades als sistemes, per tal d'analitzar-les i fer una priorització per a la seva correcció. Aquesta priorització hauria de tenir en compte factors com la severitat, grau d'afectació, facilitat de resolució, execució mitjançant poc, etc. Amb el resultat d'aquestes tasques, s'haurà de contactar amb el proveïdor responsable dels sistemes afectats per donar-li la informació i suport per a la seva resolució.
  Aquestes accions son complementàries a les ja realitzades de manera automàtica amb els escanejos recurrents.

- Consulta de l'historial d'anàlisi de cada actiu i informació associada a l'actiu
  Cal poder consultar l'historial d'escanejos de cada actiu, que ha de tenir associat el llistat de registres d'anàlisi que ha sofert, per orde cronològic i amb la possibilitat de ser descarregats pel personal autoritzat. Consulta dels inventaris d'actius (CMDB, SSCM, Exchange, MDM, entre d'altres), i del Catàleg d'Amenaces i Catàleg de vectors d'atac de l'Agència per tal de contrastar les versions de software i dels pegats aplicats en els actius o infraestructura.
  Cal conèixer la versió i els pegats aplicats a cada actiu, per tal de saber si un actiu pot estar afectat o no per una vulnerabilitat reportada pel fabricant.
  Tot i que la gestió de la CMDB no és competència d'aquest servei, sí que ha de col·laborar alimentant els camps d'informació que es generin des del servei.

- Anàlisi periòdic dels actius per trobar aquells que requereixen l'aplicació de pegats correctors.

Els actius que poden estar afectats per una vulnerabilitat han de ser analitzats per tal de saber si és necessària l'aplicació d'una actualització o pegat. Els resultats d'aquestes anàlisis han de quedar reflectits en registres basats en la plantilla genèrica especifica que es consideri.

- Anàlisi de vulnerabilitats sota demanda del client per tal de saber si un actiu necessita l'aplicació d'una actualització o pegat de seguretat.
  S'han dut a terme les anàlisis de vulnerabilitats que puguin ser sol·licitats sota demanda pels diversos serveis i organismes del client. El client serà qui indicarà quins són els interlocutors que tenen la potestat de poder sol·licitar aquest tipus de demanda.
  En cas de trobar una o vàries vulnerabilitats en el/els actiu/s, es notificaran al sol·licitat, conjuntament amb la informació referent a les mesures per solucionar aquestes vulnerabilitats.

2.2.3.6 Definició, Implementació i Manteniment de Casos d'Ús i Eines de Suport a la Detecció

- Millorar les capacitats de monitorització de seguretat i resposta a incidents
  Cal desenvolupar eines alineades amb les operacions actuals i futures per tal de que el servei de COP-SLT i COP siguin eficients i ràpids a nivell de monitorització de seguretat i resposta a incidents.

- Integració de noves fonts d'informació, definició de la taxonomia dels esdeveniments i organització per tal d'optimitzar l'eficiència del SIEM.
  S'ha de definir, mantenir i documentar una taxonomia pels diversos camps dels esdeveniments del SIEM per tal de facilitar les cerques i investigacions a la resta d'equips del SOC.
  Addicionalment, pot ésser necessari integrar noves fonts d'esdeveniments al SIEM i assegurar la correcta ingesta d'esdeveniments.

- Definició, implementació i manteniment de casos d'ús
  S'ha de definir, implementar i realitzar el manteniment i monitorització del funcionament dels casos d'ús per assegurar que els equips del SOC reben les corresponents alertes i poden realitzar les actuacions pertinents.

- Documentació de fluxes operatius i operativa interna del servei
  S'ha de documentar els fluxes operatius així com la operativa interna d'aquestes funcions per garantir la continuïtat del servei. Addicionalment també sobre totes aquelles eines desenvolupades pel servei per tal de garantir un correcte traspàs a la resta d'equips del SOC.

- Elaboració d'informes de casos d'ús i eines del servei.

- S'han d'elaborar informes a nivell tècnic i executiu del funcionament de casos d'ús, canvis en els casos d'ús i eines desenvolupades pel servei.

2.2.3.7 Característiques del Servei

2.2.3.7.1 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*:

- Coordinació amb la resta de línies de servei de l'Agència.
- Gestió de la capacitat del servei.
- Manteniment d'un portal de control on consultar l'activitat gestionada i informes generats pel servei.
- Gestió del personal (torns, vacances, etc.).
- Control i gestió dels plans de formació del personal.
- Lideratge dels aspectes de ciberseguretat recollits en l'àmbit d'actuació del servei en els diferents comitès de seguiment/crisis o problemes endegats per L'Agència o CTTI.
- Gestió i control de la informació (KDB) com procediments i instruccions operatives.
- Definició, millora i manteniment de procediments i instruccions operatives.
- Generació d'informes referents a incidències de servei, actes, informes executius, informes de resultats o informes de situació, entre d'altres, assegurant sempre la qualitat tècnica i executiva dels informes.
- Integració de l'operativa amb tercers: CTTI, per exemple.
- Suport a la resolució de conflictes i incidències operatives.
- Consulta de l'historial de tests de cada actiu, registres de test d'intrusió executats per ordre cronològic
- Pla de transformació
- Suport a la gestió tàctica i estratègica
- *Quality assurance*
- Gestió de riscos operatius del servei

2.2.3.7.2 Distribució de tasques

A continuació s'enumeren a títol enunciatiu, i no exclusiu, les principals activitats a desplegar per cada funció i nivell de servei.

Funció	Activitats	Nivell
Control i Operació de Perímetres de Seguretat	- Revisions periòdiques de patrons d'atac - Contenció de vulnerabilitats conegudes - Addició i extracció de Indicadors de Compromís (IOC) als sistemes de seguretat del perímetre. - Gestió del cicle de vida de les vulnerabilitats - Participació en la gestió de problemes de seguretat - Participació en comitès de crisi	Nivell 2

Funció	Activitats	Nivell
Gestió de perímetres de seguretat	- Definició i sol·licitud de noves regles de correlació/protecció/control sobre els actius del perímetre de seguretat com poden ser - Definició i sol·licitud per la recepció de noves alertes i sol·licitud per l'actualització (modificació/baixa) de les alertes presents - Definició de tipologies d'alertes. - Definició d'actuació - Definició i execució de protocols d'actuació	Nivell 2
Protecció en front ciberatacs	- Selecció d'esdeveniments sospitosos - Filtratge d'esdeveniments - Categorització d'esdeveniments - Priorització d'esdeveniments - Definició del que es considera un atac - Definició del procediment d'actuació principal i dels procediments d'actuació secundaris - Definició dels procediments associats als comitès de crisi - Assistència a comitè de crisi necessaris per realitzar actuacions especials o tasques d'emergència.	Nivell 2
Identificació, anàlisi i gestió de vulnerabilitats	- Programació i realització dels escanejos automàtics amb les diverses eines d'escaneig - Programació i realització dels escanejos sota demanda del client amb les diverses eines d'escaneig - Anàlisi i validació dels resultats - Assistència a comitè de crisi necessaris per realitzar actuacions especials o tasques d'emergència. - Generació dels registres de resultats - Anàlisi de vulnerabilitats sota demanda del client per tal de saber si un actiu necessita l'aplicació d'una actualització o pegat de seguretat.	Nivell 2
Identificació, implementació i manteniment de casos d'us	- Definició de casos d'ús per tots els àmbits - Implementació de la taxonomia de casos d'ús - Definició i implementació de la metodologia de casos d'ús - Definició i generació dels manuals d'operació Runbooks - Quadres de comandament de governança i operació - Manteniment dels casos d'us - Estudi de viabilitat de playbook - Implementació del playbook - Coordinar els diferents àmbits en relació casos d'ús i playbooks / runbooks. - Prioritzar integració fonts i reducció de falsos positius.	Nivell 2

2.2.3.7.3 Rols i funcions

Es descriuen a continuació els rols necessaris i les funcions assignades per tal de conformar l'equip que proporcioni els serveis, així com el perfil considerat necessari per a desenvolupar-ho.

Rols identificats	Resum Funcions	Perfil mínim considerat
Líder tècnic gestor del servei.	- Gestió de la capacitat del servei. - Gestió de riscos operatius del servei - *Quality assurance* - Definició i execució de plans de transformació - Suport a la gestió tàctica i estratègica - Suport a la resolució de conflictes i incidències operatives. - Coordinació amb la resta de línies de servei de l'Agència. - Gestió del personal (torns, vacances, etc.). - Control i gestió dels plans de formació del personal. - Lideratge dels aspectes de ciberseguretat recollits en l'àmbit d'actuació del servei en els diferents comitès de seguiment/crisis o problemes endegats per l'Agència o CTTI. - Integració de l'operativa amb tercers: oficines de seguretat de l'àmbit, proveïdors que gestionen seguretat dins entitats de l'àmbit per exemple. - 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. - Generació de lliurables executius.	Expert en vulnerabilitats
Expert en amenaces	• Recopilació i anàlisi de les ciberamenaces externes i d'altres serveis d'operacions. - Consulta de registres de les operacions dels serveis de Prevenció, Protecció i Resposta. - Interpretar la informació de ciberamenaces, relacionar-ho amb les vulnerabilitats presents al perímetres i calcular el grau d'exposició. - Proposar i executar mesures correctives per mitigar el nivel d'exposició, prioritzant segons el context (VIP, SIC, entitat, tecnologia, històric...). - Asistencia a comitès de crisis. • Anàlisi d'esdeveniments presents i passats a la cerca d'anomalies, tendències i categorització d'esdeveniments, amenaces. • Anàlisi de les eines de compartició d'amenaces. Gestió i seguiment dels tiquets de petició. • Relació entre vulnerabilitats i estat de protecció. • Proposta de tasques per la reducció del grau d'exposició • Coneixement del context de l'abast (VIP, SIC, entitat, tecnologia, històric...) per entendre la exposició davant amenaces. • Oferir suport als comitès de crisi.	Expert en amenaces

Rols identificats	Resum Funcions	Perfil mínim considerat
Analista senior	• Gestió d'esdeveniments de seguretat • Coordinació de nivells inferiors • Proposta de nous casos d'us al SIEM i protocols d'actuació • Elaboració de procediments d'actuació enfront d'atacs i casos d'us. • Definició i sol·licitud per noves alertes i sol·licitud per l'actualització (modificació/baixa) de les alertes presents. • Proposta de noves regles als elements de seguretat per millorar la detecció i protecció. • Anàlisi d'esdeveniments presents i passats a la cerca d'anomalies, tendències i categorització d'esdeveniments com a atacs. • Gestió i seguiment dels tiquets de petició. • Gestió i seguiment de les peticions d'actuació d'altres serveis. • Identificació i proposta d'industrialització del servei i millores d'evolució.	Expert en vulnerabilitats

Rols identificats	Resum Funcions	Perfil mínim considerat
Expert en vulnerabilitats	• Escanejos de vulnerabilitats d'infraestructura i aplicació. - Definició d'un calendari d'escanejos. - Definició de la prioritat d'escanejos. - Actualització del llistat d'actius a escanejar. - Gestió de l'execució dels escanejos automàtics amb les diverses eines d'escaneig. - Realització dels escanejos sota demanda del client amb les diverses eines d'escaneig. - Anàlisi i validació dels resultats - Consulta de l'historial d'escanejos de cada actiu. - Generació de registres de resultats - Gestió del cicle de vida de les vulnerabilitats. • Administració dels canals d'entrada del servei. - Gestió i seguiment dels tiquets de petició. - Gestió i seguiment de les peticions d'actuació d'altres serveis. - Administració de finestres per a l'execució d'anàlisi. • Comprovació de la correcta aplicació de les accions correctores. • Anàlisi de vulnerabilitats sota demanda del client per tal de saber si un actiu necessita l'aplicació d'una actualització o pegat de seguretat. • Sol·licitud d'aplicació de les accions correctores/pegats indicats pels fabricants. • Anàlisi periòdic dels actius per trobar aquells que requereixen l'aplicació de pegats correctors • Consulta dels inventaris d'actius (CMDB, SSCM, Exchange, MDM, entre d'altres), i del Catàleg d'Amenaces i Catàleg de vectors d'atac de l'Agència per tal de contrastar les versions de software i dels pegats aplicats en els actius o infraestructura. • Consulta de l'historial d'anàlisi de cada actiu • Identificació i proposta d'industrialització del servei i millores d'evolució.	Expert en vulnerabilitats

Rols identificats	Resum Funcions	Perfil mínim considerat
Expert en gestió d'atacs i incidents autogestionats (N2)	• Elaboració de procediments d'actuació enfront d'atacs - Definició de la categorització dels atacs - Definició de la prioritat d'actuació sobre cada atac tenint en compte el valor dels actius afectats - Definició del procediment d'actuació principal i dels procediments d'actuació secundaris - Definició dels procediments associats els comitès de crisi en cas d'atacs de gran afectació. - Generació d'informes de resultats de l'actuació sobre un atac • Recepció d'alertes del perímetre (SIEM, Splunk, IPS, antivirus, MDM, etc.) i ampliació de cobertura del perímetre - Definició de tipologies d'alertes. - Definició d'actuació. • Revisió d'alertes en temps real amb operacions predefinides • Suport a la gestió en la generació de lliurables tècnics i executius. • Proposta millores de detecció i protecció en eines de Ciberseguretat • Identificació i proposta d'industrialització del servei i millores d'evolució. • Coordinació amb la resta de l'equip.	Expert en gestió d'atacs I incidents autogestionats (N2)
Expert definició i manteniment de casos d'us	• Millorar les capacitats de monitorització de seguretat i de resposta a incidents. • Integració de fonts i definició de taxonomia i organització dels esdeveniments per optimitzar l'eficiència i facilitat de cerques al SIEM. • Definició, implementació i manteniment de casos d'us. Per fonts noves i existents. • Manteniment de l'inventari de casos d'ús. • Monitorització dels casos d'ús i creació d'informes d'ús de cadascun d'aquests. • Millora dels processos i les operacions dels analistes creant quadres de comandament, informes o altres eines d'investigació similars. • Millorar l'eficiència de la monitorització de seguretat i de la resposta a incidents. • Documentació de fluxes operatius en relació l'elaboració de casos d'ús. • Elaboració d'informes a nivell tècnic i executiu de tasques que impliquin els casos d'ús.	Expert en amenaces

2.2.3.7.4 Volumetries esperades

Aquest servei es centrarà principalment en l'operativa dels hospitals, tot i que pel caràcter transversal de moltes aplicacions i sinergies d'aquesta funció por haver-hi actuació amb altres conceptes d'aquesta taula, encara que haurien de ser mínims.

Per proporcionar una referència aproximada per al correcte dimensionament del servei es proporcionen algunes dades de volumetries aproximades mensuals esperades en funció a les

actuals. Aquestes volumetries es poden veure incrementades segons es vagin afegint perímetres, eines o oficines.

Concepte	Quantitat
Control i Operació de Perímetres de Salut	
Alertes gestionades	4.000
Eines dels perímetres	400
Actius Analitzats	5.000
Vulnerabilitats tractades	39.000
Aplicacions	2.500
Adreces IP en Sistemes d'Informació	5.000
Llocs de treball	+100.000
Entitats de l'àmbit de Salut	161

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.

2.2.3.7.5 Lliurables dels serveis

La prestació del servei de Control del Perímetre requereix, addicionalment, la preparació d'una sèrie de lliurables, els quals es poden considerar informes sobre l'estat de les infraestructures, resums de l'activitat dels serveis, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, notificacions, mètriques i indicadors, entre d'altres.

2.2.3.7.6 Documents

El llistat que es mostra a continuació, és un mostra dels documents clau que s'han de lliurar per servei i indicant la periodicitat:

Servei	Document	Periodicitat
Control i Operació de Perímetres de Seguretat	Informe de la seguretat dels sistemes transversals	Mensual
	Informe de seguretat dels sistemes d'informació.	Mensual
	Informe de seguretat de les persones.	Mensual
	Informe d'estat de situació	Diari
	Informe de seguretat i de la navegació per entitat	Mensual
	Informe de la seguretat en el lloc de treball	Mensual
	Llistat casos d'ús i playbooks associats.	Mensual
	Inventari d'eines operades i periodicitat de revisió	Mensual
	Llista i estat de peticions demanades a evolució	Mensual
	Estat del nivell de seguretat dels àmbits adherits al servei d'operació de perímetres	Mensual
	Informe de comptes compromesos	Mensual
	Informe de campanyes d'Spam i Phishing	Mensual
	Pla manual de correcció de vulnerabilitats	Mensual
	Pla manual de protecció de vulnerabilitats	Mensual
	Seguiment mensual dels casos d'ús	Mensual
	Informe mètriques correu	Trimestral

	Mètriques Phishing i Comptes Compromesos	Trimestral
	Mètriques Comptes Compromesos	Trimestral
	Seguiment de Vulnerabilitat Pla de Resolució	Trimestral

2.2.3.7.7 Mètriques i indicadors

Entre els diferents lliurables a definir pel servei, s'haurà de ser capaç de calcular i facilitar a la capa de "gestió de les operacions", encarregat 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. L'Agència es reserva el dret de modificar aquesta llista de mètriques.

Mètriques de Control i Operació de Perímetres de Seguretat

Mètrica	Descripció
Activitat Gestionada	Nombre de tiquets gestionats pel servei i tipologia de les peticions
Tipus de Peticions	Indica el tipus de tiquets gestionats (peticions, incidències, canvis,…)
Escalat de Peticions	Indica les tasques realitzades que han estat delegades o escalades a altres serveis
Demanda Actual Serveis	Indica el nombre de tiquets actualment oberts i l'estat en el que es troben per cadascuna de les cues de servei
Temps mig de resolució	Temps mig de resolució de peticions per servei mensualment
Peticions d'actius crítics	Numero de peticions relacionades amb actius crítics per servei i mes
Pla de Capacitat	Càlcul de la capacitat dels serveis del soc en funció de les tasques realitzades per cada servei
Estadístiques d'alertes per entitat.	Total de les alertes classificat per entitat i severitat.

Mètrica	Descripció
Evolució de les alertes durant tot el mes	Gràfica on es veu l'evolució del volum d'alertes blocades automàticament.
Estadístiques sumatori per franja horària	Gràfica on es veu l'evolució del volum d'alertes blocades, tant manuals com automàtiques.
Principals alertes blocades manualment	Gràfica amb el TOP d'alertes que es bloquegen manualment.
Estadístiques atacs	Volumetria d'alertes total, gestionades i classificades per tipologia, severitat, entitat, etc
Connexions blocades per entitat	Gràfica tràfic de navegació blocat per entitat.
TOP 10 SICs Atacats	TOP dels actius crítics de l'àmbit atacats, que mostra la seva nomenclatura i la volumetria total.
TOP 10 Atacs pels TOP de SIC	TOP de actius crítics, que mostra el TOP 5 dels atacs rebuts.
Numero de vulnerabilitats detectades i corregides als sistemes d'informació	Volumetria classificada per entitat i entorn.
Numero de mesures de protecció aplicades.	Volumetria classificada per tipologia, entitat i entorn.
Numero de vulnerabilitats detectades i protegides	Volumetria classificada per tipologia, entitat i entorn.

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 per exemple:

- Nombre de tiquets gestionats pel servei per tipologia
- Total hores dedicació en el servei
- Total d'anàlisi realitzades pel servei
- Nombre d'incidències i peticions resoltes segons taula de prioritat en el període
- Total d'incidències i peticions resoltes en el període
- Dates d'inici i de lliurament pactat i real de projectes
- Admissions i desvinculacions de personal presencial en el període

- Puntuacions de les enquestes de satisfacció de lliurables

3 Condicions d'execució del servei

3.1 Elements a tenir en compte per la prestació del servei

De tot el que s'ha exposat prèviament es pot observar els següents elements essencials del contracte:

- S'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, execució d'anàlisi de seguretat, correcció i seguiment de vulnerabilitats, resolució d'infeccions de lloc de treball, integració amb el Centre de Control, integració amb l'equip SAU CTTI, equips locals de les entitats hospitalàries...), així com canalitzar les comunicacions necessàries per a les vies i eines establertes.

- S'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.

- Un model de govern que: (i) garanteixi que els analistes de N2 liderin l'estratègia de desplegament de la seguretat (ii) identifiqui de forma clara el rol de gestió del servei.

- L'existència de lliurables, el contingut i la periodicitat dels quals és preceptiva, així com la presentació d'aquells informes que l'Agència consideri pertinents.

- Propostes de millores en el servei que tinguin com objectiu augmentar el nivell de maduresa de cadascun dels serveis així com millorar l'eficiència de l'activitat operativa en el temps, aconseguint així la capacitat de gestionar més esdeveniments amb els mateixos recursos.

- S'ha d'incloure en el preu de servei i per tant no tindran impacte econòmic les actuacions que derivin de fins a cinc operatius anuals. En cas que l'Agència requereixi de l'adjudicatari l'execució de serveis en més de cinc operatius, aquell podrà facturar els serveis prestats a partir del sisè operatiu.
- El plantejament d'equips humans i la seva organització haurà de donar resposta a les necessitats i les funcions que l'Agència demana amb el detall de dedicacions i perfils corresponents.

- Ser capaç de donar resposta a un increment significatiu de les volumetries (fins 50%) durant la durada del contracte sense cost addicional.

- Millorar i completar les mètriques senyalades.

3.2 Modalitat de prestació del servei

Un servei enfocat en perfils de nivell 2 (N2) per a les tasques de Control i Operació dels Perímetres de Seguretat en l'àmbit de Salut.

El servei haurà d'incloure un **equip d'especialistes de seguretat (N2)** amb els perfils indicats a l'apartat 2.4 – *Rols i Funcions*, encarregats de dur a terme les tasques operatives i especialitzades definides per al servei, així com de la **gestió, orientació tècnica i governança operativa** dins del seu àmbit d'actuació.

Aquest equip actuarà com a **nivell únic dins de la present licitació**, sense disposar d'un nivell 1 associat al contracte, però interrelacionant-se amb el nivell 1 del COP Core, així mateix mantenint la capacitat de **coordinació i escalat amb altres serveis o nivells superiors i inferiors existents**, si s'escau.

La proposta haurà de **detallar l'estructura del servei N2**, així com el **model de treball, responsabilitats i funcions específiques** a desenvolupar dins del marc operatiu i tecnològic del servei de perímetre en l'àmbit de Salut. Igualment, caldrà exposar la **capacitat d'adaptació, disponibilitat i cobertura del servei**, tot garantint que aquest pugui donar resposta a la demanda actual i permetre un creixement escalable del servei en el futur.

Amb independència del model organitzatiu proposat, l'adjudicatari haurà de destinar com a mínim una persona a actuar com a **cap de servei**, encarregat de dirigir i gestionar la relació del contracte i el servei de l'adjudicatari amb l'Agència. A aquest efecte, 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.
- 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.
- Planificar l'activitat i mantenir la informació dels plans de capacitat.
- Assegurar una bona col·laboració entre els diferents agents implicats en la prestació de serveis als clients de l'Agència.

3.3 Horaris

Els serveis s'hauran de prestar d'acord amb els horaris de la taula següent.

BLOC DE SERVEI	HORARI DE PRESTACIÓ

COP-SLT (N2)	12x5 dies laborals amb guàrdies

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.

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.

3.4 Localització física.

El servei haurà de ser prestat des de les oficines de l'adjudicatari, tot i que un cop iniciada la prestació, si així ho decideix l'Agència, es podrà realitzar part en remot. Les oficines de l'Agència estan ubicades a l'Hospitalet de Llobregat, lloc on s'haurien d'ubicar els equips prestataris en cas que l'Agència requereixi la presencialitat. Davant d'aquesta situació, la presencialitat a les oficines hauria de ser inferior a 45 minuts un cop demanada la presencialitat.

Addicionalment, s'ha de contemplar la possibilitat de que part d'aquests serveis requereixin del desplaçament dels professionals a les instal·lacions dels clients de l'Agència que poden estar ubicades a qualsevol part del territori de Catalunya. Aquesta situació no comportarà cap cost addicional per l'Agència.

Al llarg del contracte es podria requerir un canvi en la ubicació dels professionals entre els centres operatius de l'Agència, 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.

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

3.5 Equip Humà i Perfils

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 esquema 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.

Els licitadors hauran d'incloure en la seva proposta l'organigrama i esquemes d'equips per tal de donar resposta a les necessitats expressades en aquest plec, incloent, i de forma nominal, el/les persones designades com a cap de servei i d'altres figures rellevants segons la proposta del licitador.

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:

BLOCS DE SERVEI	EQUIP	DIMENSIONAMENT MINIM (HORES ANUALS)
Bloc de Servei Recurrent -7 FTE al 100% de dedicació-	Control i Operació del Perímetre N2	12.320
Bloc de Servei No Recurrent	Control i Operació del Perímetre N2	3.520
Total		15.840

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

Durant la vigència d'aquest plec, es podran demanar un increment de dedicació o augment del número de perfils per un total de 3.520 hores com a part del bloc de servei extraordinari. Moment en el que s'indicaria els perfils requerits.

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

Control i Operació del Perímetre inicial	DISTRIBUCIÓ ORIENTATIVA
Líder tècnic gestor del servei	14,3%
Expert en amenaces	14,3%
Analista sènior	14,3%
Expert en vulnerabilitats	14,3%
Expert en gestió d'atacs i incidents autogestionats.	14,3%
Expert definició i manteniment de casos d'us	28,5%

3.6 Perfils

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

Perfil	Requisits
Expert en vulnerabilitats	5 anys o més d'experiència demostrable exercint les següents funcions: • Pentesting i anàlisi de vulnerabilitats. • Anàlisi de resultats de pentesting i vulnerabilitats per tal de conèixer les seves implicacions. • Metodologies d'intrusió / pentest (OSSTM, OWASP). • Elements de seguretat de les principals tecnologies de cloud computing. • Alt grau de coneixement i experiència en tècnica operativa de Sistemes d'Informació heterogenis, xarxes, softwares, protocols de comunicacions, etc. • Vulnerabilitats i debilitats tècniques més freqüents, així com la seva explotació, incloent-hi problemes de seguretat física, errors de disseny en protocols, programari maliciós, errors d'implementació, debilitats de configuració, errors o indiferència dels usuaris, entre d'altres, així com solucionar-los o definir accions mitigadores, o de contenció. • Gestió d'equips i definició de procediments per la realització d'escanejos i test de penetració. • Capacitat proactiva, resolutiva i dots de lideratge.
Expert en amenaces	• Titulat universitari en informàtica, telecomunicacions o similars en l'àmbit TI. 5 anys o més d'experiència demostrable en els següents punts: • Definició i millora de processos. I eines de reporting i quadres de comandament. • Tecnologies aplicades a centres de processament de dades. • Capacitat per l'execució de tasques procedimentades i de gestió. • Tasques d'atenció al client. • Tècniques de seguretat de xarxes, incloent-hi seguretat perimetral (disseny, filtratge de paquets, sistemes proxy, xarxes desmilitaritzades, protecció d'entorn de sistemes i altres), seguretat d'encaminadors, monitoratge de tràfic, entre d'altres. • Anàlisi de resultats de pentesting i vulnerabilitats per tal de conèixer les seves implicacions. • Coneixements avançats de la majoria de sistemes operatius, bases de dades, softwares de control, softwares de treball, en especials els utilitzats pel client. • Tractament d'esdeveniments de seguretat, entre d'altres. • Elements de seguretat de les principals tecnologies de cloud computing. • Creació manual de signatures de detecció i cerca de patrons a les eines perimetrals. • Metodologies de treball amb les eines de monitoratge, protecció perimetral on premise i cloud (SIEM, Splunk, IPS, antivirus, DLP's, MDM's, CASB), principalment, aquells que utilitza el client. • Nivell alt o mitjà d'anglès.

Perfil	Requisits
Expert en gestió d'atacs i incidents autogestionats (N2)	5 anys o més d'experiència demostrable en els següents punts: • Tècniques de seguretat de xarxes, incloent-hi seguretat perimetral (disseny, filtratge de paquets, sistemes proxy, xarxes desmilitaritzades, protecció d'entorn de sistemes i altres), seguretat d'encaminadors, monitoratge de tràfic, entre d'altres. • Anàlisi de resultats de pentesting i vulnerabilitats per tal de conèixer les seves implicacions. • Sistemes operatius, bases de dades, softwares de control, softwares de treball, en especials els utilitzats pel client. • Tractament d'esdeveniments de seguretat, entre d'altres. • Elements de seguretat de les principals tecnologies de cloud computing. • Creació manual de signatures de detecció i cerca de patrons a les eines perimetrals. • Metodologies de treball amb les eines de monitoratge, protecció perimetral on premise i cloud (SIEM, Splunk, IPS, antivirus, DLP's, MDM's, CASB), principalment, aquells que utilitza el client. • Gestió d'equips i definició de procediments de seguretat i actuació enfront d'atacs, entre d'altres. • Capacitat proactiva, resolutiva i dots de lideratge.

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

3.7 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.

3.8 Control de rotació

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

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

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

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

3.9 Eines i equipament per a la prestació de serveis.

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

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

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

L'Agència no proveirà:

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

En conseqüència, els adjudicataris hauran de:

- Subministrar tots elements de maquinari, programari i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments de l'objecte del contracte. Aquests elements seran ***d'ús exclusiu*** pels serveis prestats a l'Agència i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.

- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.
- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip de Mitjans Tècnics de l'Agència.

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

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

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

3.10 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.

3.11 Seguretat Corporativa

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

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- Facilitar l'accés en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de l'Agència (sigui o no per l'exercici de la seva funció).
- Acceptar les normes i polítiques que estableix l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.

- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'àrea de Mitjans Tècnics per fer el desplegament de polítiques i controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.
- Els equips, així com la informació resident dels mateixos serà sempre custodiada per l'Agència.
- Garantir l'estabilitat dels equips (reduint al mínim la rotació de personal).
- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (ENS, LOPDGDD, GDPR, LSSI, etc.).

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

3.12 Control de Gestió

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

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

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

3.13 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

3.14 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.

3.15 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.

3.16 Seguretat

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

3.16.1 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.

3.11.1. 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.

3.11.2. Compliment del marc legal de ciberseguretat i del marc normatiu intern

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

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

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

3.11.3. Capacitat tècnica

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

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

3.11.4. Adquisició de productes/eines i productes o serveis de seguretat

Tant en el cas que es desenvolupin productes/eines, es facin integracions amb altres eines o s'adquireixin eines de mercat o qualsevol component de sistemes d'informació (hardware, software, etc.), aquests hauran de ser compatibles amb l'arquitectura de seguretat de l'Agència i complir amb els requeriments de seguretat que estableixi el marc legal i el marc normatiu intern, sotmetre's a proves tècniques de seguretat i aplicar les correccions necessàries prèviament a la posada en producció del producte/solució/eina. Caldrà incorporar el producte/eina dins el procés de desenvolupament segur de l'Agència de Ciberseguretat des de la fase de disseny fins a la posada en producció.

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

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

3.11.5. Interconnexions

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

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

3.11.6. Verificació del compliment i auditoria

L'Agència es reserva el dret a verificar i auditar, amb mitjans propis o de tercers, el compliment de les mesures de seguretat requerides en base al marc legal de ciberseguretat i al marc intern per als sistemes d'informació emprats per a l'execució del contracte, en el moment i amb la periodicitat que s'estimi convenient. L'Agència podrà requerir el seguiment dels plans d'acció derivats d'aquestes verificacions i auditories. L'empresa adjudicatària del contracte basat haurà de disposar dels

recursos adients per a dur terme l'execució de les tasques que li corresponguin en relació a aquest model de compliment, donant resposta en els terminis marcats per l'Agència de Ciberseguretat. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència de Ciberseguretat.

3.11.7. Incidents de seguretat

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

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

3.11.8. Accés a la informació

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

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

3.17 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.

3.18 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.

3.19 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.