Plec de prescripcions tècniques particulars que regeix la contractació basada relativa al Servei de suport a la funció de Resposta Activa en l'àmbit sanitari

Exp. CB25AMOPL3001

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 alt nivell d'activitat de gestió. Més concretament, el nombre de ciberatacs rebuts durant l'any 2023 va ser de més de 5.000 milions, en contraposició als 4.400 milions d'atacs del 2022. Pel que fa als incidents de seguretat, l'Agència en va gestionar prop de 2.670 durant el 2023, en comparació amb els 2.175 de l'exercici anterior.

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

.

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.

2 Antecedents

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).

3 Descripció dels serveis objecte de la contractació basada.

3.1 Context dels serveis objecte de la licitació.

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

Concretament s'emmarca en el Lot 3 de Resposta a Incidents

Dins d'aquest lot s'inclouen, tal i com indica el Plec de Clàusules Tècniques de l'Acord Marc de referència:

- **Resposta a incidents** : Funció responsable de respondre de forma diligent a incidents de seguretat en temps i forma, minimitzant l'impacte, assegurant-ne l'erradicació i garantint que no es puguin tornar a repetir de la mateixa manera. Per això s'encarregarà de tota la coordinació de la crisi, així com de proveir el relat necessari respecte a la investigació per a la presa de decisions en el context d'un incident . Les tasques de la funció inclouen, entre d'altres: Recopilació i ordre cronològic de tota la informació i evidències generades, coordinació dels diferents equips participants a la resposta d'incidents, gestió i lideratge dels diferents comitès de crisi. Tanmateix, inclou totes les tasques de preparació adients per garantir que tant els àmbits d'actuació com el propi equip de resposta, disposen de les capacitats necessàries per respondre davant d'incidents de manera efectiva i eficient.

- **Anàlisi forense :** En aquesta funció s'executaran les diferents anàlisis tècniques derivades d'incidents o campanyes de cerca proactiva d'amenaces per reduir l'impacte en cas d'incident, determinar les causes d'un incident per evitar que es pugui tornar a repetir i proveir el context necessari que ajudi a la presa de decisions als diferents comitès. Per això haurà de recopilar, analitzar i emmagatzemar les evidències seguint un procés que garanteixi la integritat d'aquestes i de la seva cadena de custòdia garantint-ne la validesa davant un possible procés judicial. Això inclou tasques com: anàlisi de codi maliciós, anàlisi forense de diferents tipus de dispositius i tecnologies, proposta de plans d'erradicació i recuperació en el context d'un incident, extracció d'indicadors sobre la base de l'anàlisi forense, inventariat i control de les evidències recol·lectades, així com el registre i documentació dels resultats de les investigacions realitzades.

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

- **Simulacres d'incidents i exercicis de preparació:** En aquesta funció es realitzaran sessions de simulacres amb l'objectiu de avaluar i conèixer el grau de preparació enfront incidents (*Incident Readiness*) de les diferents entitats dins de l'ambit d'actuació del presente contracte. Les tasques a desenvolupar inclouen, entre d'altres, el desenvolupament i disseny d'escenaris per a la realització de simulacres amb sinèrgies o relació amb els punts a avaluar,

la definició d'exercicis i activitats per a la mesura de les capacitats de resposta de la entitat, o la consolidació de les dades extretes d'aquests exercicis.

De totes les àrees que formen l'Agència de Ciberseguretat de Catalunya, l'Àrea d'Operacions, s'encarrega d'executar mesures operatives específiques per prevenir la materialització de les ciberamenaces dins dels àmbits d'actuació i de respondre, quan sigui necessari, per a reduir al màxim la seva afectació si l'incident arriba a materialitzar-se.

Per dur a terme aquestes funcions, l'Àrea d'Operacions disposa d'un model de seguretat anomenat perímetre de seguretat. El perímetre de seguretat es defineix com 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.

Els serveis objecte de la present licitació s'emmarquen a la vertical d'Intel·ligència i Resposta de l'Àrea d'Operacions. El servei de Resposta Activa té l'objectiu de reduir en temps i forma l'afectació enfront els incidents de ciberseguretat, garantint que no tornin a succeir en les mateixes circumstàncies. Per tal de donar context sobre l'activitat gestionada pel servei objecte de la contractació basada, durant l'any 2024 s'han gestionat aproximadament 200 incidents complexos, dels quals un total de 30 han comportat la gestió d'una crisi.

Addicionalment, s'han realitzat diverses campanyes de cerca proactiva d'amenaces sobre la base de l'activitat detectada en els àmbits d'actuació de l'Agència. En total s'han realitzat 5 campanyes de cerca proactiva en entitats de diferent tipus i mida.

Per últim, durant l'any 2024 s'han realitzat simulacres i exercicis de preparació als 60 hospitals públic de Catalunya.

3.2 Serveis de suport a les funcions de Resposta Activa en l'àmbit Salut.

3.2.1 Objecte i descripció.

L'objecte de la present licitació és la contractació del servei de suport a la funció de Resposta Activa que existeix en l'Àrea d'Operacions de l'Agència, per a donar suport dins de les entitats dels àmbits hospitalari, d'atenció primària, i sociosanitari.

El servei de suport de Resposta Activa porta a terme la gestió complerta davant la materialització de les ciberamenaces, la gestió d'incidents de ciberseguretat, investigació, anàlisi forense, i execució dels processos que s'hi puguin derivar com pot ser la identificació de millores o també d'incompliments normatius. Tanmateix, també inclou les tasques relacionades amb la preparació i avaluació de las diferents entitats de l'àmbit d'actuació davant d'aquests mateixos incidents.

Addicionalment, el servei licitat desenvolupa i executa missions de recerca proactiva d'incidents per identificar amenaces latents que s'han materialitzat en l'entorn quan la resta de mecanismes de seguretat han estat incapaços de detectar.

Les subfuncions del servei de suport de Resposta Activa són les següents:

- Gestió d'incidents
- Cerca proactiva d'incidents
- Gestió d'evidències
- Avaluació de les capacitats de resposta

Amb l'objectiu de dur a terme satisfactòriament el servei que dona suport a aquestes subfuncions, es desenvoluparan les accions mínimes que s'espera de la empresa que resulti adjudicatària en els següents apartats.

3.2.2 Objectius generals del servei

El present apartat inclou un llistat d'objectius generals del servei que es requereix haver assolit a la finalització del contracte adjudicat. Aquest llistat defineix el criteri que permet avaluar el grau de compliment del objecte de la present licitació, segons l'orientació cap a resultats que s'espera del servei adjudicat:

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

- El servei focalitzará la seva capacitat en els **incidents complexos.** La resta seran governats i la seva operació recau sobre altres equips, com els de la funció de Control i Operació de Perímetres proveïdors dels diferents àmbits d'actuació de la l'Agència.
- El servei ha de garantir que les entitats dels seus àmbits d'actuació estan **contínuament preparats** per poder dur a terme la resposta a incidents. Així mateix ha de assegurar la capacitat de mesura de les diferents capacitats de resposta d'aquestes entitats.
- Donat l'abast i l'àmbit d'actuació, el servei ha **d'especialitzar-se en l'entorn** assegurant la disponibilitat, manteniment i articulació de la informació de **context disponible** de cadascuna de les entitats per a agilitzar les accions de resposta davant un incident de ciberseguretat.
- De la mateixa manera**,** el servei ha de **desenvolupar les tàctiques** (processos, mitjans, noves capacitats) per habilitar la resposta en temps i forma davant incidents.
- El servei ha de reduir el cost de la resposta a incidents mitjançant **l'automatització i la innovació.**
- El servei ha de ser **completament autosuficient** amb capacitat de lideratge i de defensar els interessos de l'Agència.
- El servei ha de **col·laborar i coordinar-se** amb altres equips de diferents àmbits amb la mateixa funció.
- El servei ha de donar suport a l'Agència en el **posicionament internacional** del CATALONIA-CERT, com a referent de ciberseguretat.

El licitador ha d'incloure a la seva proposta una descripció detallada de la seva estratègia d'assoliment dels objectius definits anteriorment (afegint una planificació associada), per cadascun dels àmbits d'actuació. La proposta ha d'incloure una planificació associada, detallant el calendari de fites a assolir, els nivells d'assoliment que s'espera aconseguir en cada cas i el mecanisme de càlcul del grau d'assoliment de cada objectiu. Es tindrà en consideració la viabilitat del pla proposat, la reducció dels temps requerits per assolir els objectius i la millora qualitativa d'aquests mateixos objectius.

3.2.3 Activitats i funcionalitats del servei

3.2.3.1 Gestió d'incidents

La subfunció de Gestió d'Incidents és l'encarregada de dur a terme les activitats necessàries per a articular i garantir la resposta diligent davant un incident de seguretat en totes les seves fases. Dins d'aquesta subfunció s'identifiquen, entre d'altres, les següents funcionalitats:

a) **Resposta a incidents de forma diligent amb l'objectiu de garantir uns àmbits d'actuació protegits.**

El servei de suport haurà de desenvolupar les següents accions dins del cicle de gestió d'un incident, sempre seguint models estàndards i metodologies reconegudes internacionalment com per exemple NIST 800-61.

- **Preparació de les eines i informació de context disponible.**

Cal disposar de la preparació necessària per a poder dur a terme la resposta a incidents. En aquest sentit l'equip de Resposta Activa ha de disposar i tenir preparades en tot moment, les eines necessàries per a poder donar resposta a l'incident, com poden ser, entre altres, les diferents eines de triatge, les aplicacions o solucions per a investigar i compartir dades, etc.

Així mateix, l'equip ha de disposar i articular de forma àgil i precisa la informació de l'entorn disponible amb l'objectiu de tenir el màxim context possible en el contacte inicial per a agilitzar les accions i millorar la visibilitat sobre l'incident, aquesta informació pot ser la relativa al nombre de màquines, tecnologies disponibles en l'entitat afectada, matriu d'escalats i contactes, etc.

- **Recopilació de tota la informació associada a l'incident.**

Cal recopilar i ordenar cronològicament tota la informació que es té de l'incident, incloent-hi la informació i troballes generades provinents de tercers, el propi afectat o d'altres equips com ara la funció de Control i Operació del Perímetre de Seguretat o d'Intel·ligència Operativa.

Els incidents de seguretat han d'estar tipificats segons el els models de categorització de l'Agència.

- **Definició de la prioritat de tractament dels incidents.**

En cas que tingui lloc un nombre d'incidents simultanis que superi les capacitats de l'equip de resposta enfront d'incidents, cal definir una prioritat que s'establirà segons la criticitat dels actius implicats, la informació que es pot veure compromesa o l'alteració de l'operativa de negoci que pot veure's afectada.

- **Anàlisi de la informació i de les evidències recopilades.**

Cal portar a terme l'anàlisi de les evidències i de la informació obtinguda, per tal de respondre preguntes com ara el vector d'entrada inicial, els mecanismes de persistència emprats, els moviments laterals realitzats o la informació extreta des de l'afectat.

- **Definir i aplicar accions de contenció per tal de bloquejar o mitigar l'afectació d'un incident.**

Aquestes accions han d'anar encaminades a contenir l'incident de forma temporal i proveir una finestra de temps per tal que l'equip d'investigació pugui analitzar la informació i les evidències, definir una línia d'actuació i dur-la a terme per tal de solucionar l'incident de forma permanent.

Les accions de contenció han d'adequar-se a la situació de l'incident i a la seva criticitat, i han de ser controlades i registrades adientment.

Un cop s'ha solucionat l'incident, cal fer el seguiment de les accions de contenció per tal de revertir aquells canvis que puguin ser negatius per l'operativa dels clients del l'Agència.

En cas que alguna o vàries d'aquestes accions de contenció o reversió dels canvis s'hagin de dur a terme per equips que no formen part del servei, cal definir clarament el mètode/canal de notificació a tercers, el format del contingut de la petició i els interlocutors que duran a terme aquesta comunicació per totes les parts. L'equip ha de validar aquesta sol·licitud amb les terceres parts afectades, per tal d'arribar a un format de petició d'accions alineat per totes les parts.

- **Definició de la línia d'actuació per afrontar l'incident.**

Cal definir una línia d'actuació per tal de gestionar l'incident. Aquesta definició ha de contenir, com a mínim, l'ordre d'actuació, les accions a efectuar i els encarregats de portar a terme aquestes accions així com els seus rols i responsabilitats.

En cas que alguna o vàries d'aquestes accions s'hagin de dur a terme per equips que no formen part del servei cal definir clarament el mètode/canal de notificació a aquestes terceres parts, el format del contingut de la petició i els interlocutors que duran a terme aquesta comunicació per totes les parts. L'equip ha de validar aquesta sol·licitud amb les terceres parts afectades, per tal d'arribar a un format de petició d'accions alineat per totes les parts.

- **Execució de les accions d'actuació per afrontar l'incident.**

S'han de dur a terme les accions d'actuació prèviament definides. En cas que sigui necessària la comunicació amb terceres parts, per tal que duguin a terme certes accions, aquesta notificació es farà segons les definicions prèviament acordades i segons l'ordre d'actuació definit.

La resolució dels incidents per part de l'equip de Resposta Activa s'ha d'adequar als temps de resposta mínims definits per l'Agència. En cas de detectar objectivament una manca de capacitat i/o recursos per poder dur a terme aquesta resolució en temps definit, s'ha d'informar al responsable del servei per part de l'Agència, i en cas que aquest ho consideri oportú, han de dur a terme les mesures de reforç compensatòries necessàries perquè el temps de resolució no es vegi afectat.

- **Monitoratge i revisió dels resultats de les accions d'actuació, i estat de l'incident.**

De forma paral·lela i immediatament posterior a les accions d'actuació enfront de l'incident, s'han de monitorar els resultats d'aquestes i comprovar si han tingut èxit en bloquejar, repel·lir o mitigar l'incident. Addicionalment, cal comprovar si s'ha materialitzat alguna afectació del servei als actius on s'han aplicat les esmentades accions.

Si les accions dutes a terme no han tingut els resultats esperats, cal tornar a realitzar l'anàlisi de la informació i de les evidències disponibles, així com dels resultats obtinguts de l'aplicació de la línia d'actuació, per tal de redefinir una nova línia d'actuació.

- **S'han de desplegar les mesures adients per recuperar els incidents.**

Aquestes mesures han d'estar dirigides a protegir la infraestructura afectada davant l'incident actual i/o futurs incidents del mateix tipus, per tal de evolucionar la seguretat dels sistemes per tal de que no es torni a produir.

Per implementar aquestes mesures s'ha de contar tant amb la resta d'equips disponible a l'Àmbit, tant interns com externs.

- **Emetre recomanacions i propostes de millora per que l'incident no es torni a produir.**

Els resultats de la resposta enfront d'incidents han de ser analitzats per tal d'obtenir mesures que permetin millorar la "postura de seguretat" de l'àmbit afectat i evitar que l'incident es torni a produir. Aquestes mesures s'han de comunicar a la resta de funcions involucrades.

S'ha de tenir un registre i fer un seguiment de les propostes, atenent que la no aplicació pot derivar novament en que succeeixi el mateix tipus d'incident.

- **El servei ha de tenir capacitat per defendre davant d'un tercer la resolució del cas, conclusions i propostes de millora, com les possibles mancances o incompliments identificats.**

- **Integrar-se en la gestió d'incidents amb altres equips operatius de la mateixa naturalesa**

Davant la transversalitat de part de les infraestructures que donen servei als diferents àmbits d'actuació de l'Agència, l'equip ha de assegurar la integració operativa amb altres equips de la mateixa naturalesa que donin servei en entitats del sector públic o en qualsevol dels àmbits d'actuació de l'Agència, així siguin propis de les entitats clients o de la pròpia Agència.

b) **Garantir la preparació per a la resposta a incidents dels àmbits d'actuació de l'Agència.**

La fase de preparació enfront d'un incident de seguretat, consisteix entre altres, en la implementació del conjunt de mesures i processos proactius que permeten a una organització establir capacitats i procediments per a detectar, respondre i recuperar-se eficaçment davant incidents de seguretat. El servei licitat haurà de garantir la correcta preparació de les entitats dins del seu àmbit d'actuació.

c) **Capacitat de resposta a incidents a gran escala en entorns complexos, obsolets o no controlats.**

Els incidents en els últims anys han evolucionat cap a formes d'intrusió cada vegada més complexes. Grups cibercriminals més especialitzats realitzen atacs dirigits, a través d'intrusions manuals, on un operador es mou per la xarxa fins a trobar les conegudes com a "joies de la corona", intentat causar el major impacte possible. Atacs amb doble extorsió, indisponibilitat i fuita d'informació, o fins i tot triple extorsió quan inclouen a clients o

proveïdors de la víctima són cada vegada més freqüents. D'altra banda grups APTs, de vegades més silenciosos, persisteixen en l'àmbit durant llargs períodes de temps.

El servei licitat tindrà la capacitat de donar resposta principalment a aquests tipus d'incidents complexos, dins d'entorns on normalment les condicions per a realitzar una resposta a incidents no és idònia.

L'Agència, a més de les capacitats de laboratori propi, disposa d'una plataforma auto-continguda al núvol per la gestió d'incidents de seguretat, aquesta plataforma dota de les eines i capacitats per garantir l'execució dels àmbits clau en la gestió d'incidents (gestió i comunicació, adquisició d'evidencies, anàlisi d'evidencies, contenció de l'amença, neteja i erradicació) en qualsevol nou entorn.

d) <u>Desenvolupament de la infraestructura per poder donar resposta.</u>

Actualment, dins del SOC/CERT, ja existeix un ecosistema per a la gestió d'incidents, composat per diferents solucions tecnològiques i processos, que proveeixen les següents capacitats:

- **Gestió i comunicació:**
  - Tecnologies i procediments per a la coordinació amb tercers, compartició d'informació i seguiment dels incidents.
- **Adquisició d'evidències.**
  - Tecnologies i procediments per a l'adquisició d'evidències presencial i remot a servidors, estacions de treball i dispositius mòbils.
  - Capacitat d'emmagatzematge d'evidències en el núvol i físic en caixa forta.
- **Anàlisis d'evidències.**
  - Tecnologies per a l'anàlisi d'evidències de data lake i SIEM en el núvol i físic.
- **Contenció de l'amenaça**
  - Tecnologies de EDR, AntiDDoS i AntiSPAM en el núvol i fisc.
- **Neteja i erradicació.**
  - Tecnologies per al desplegament de solucions antivirus massivament.

Algunes d'aquestes capacitats es troben físicament en el laboratori de l'Agència i en el núvol.

El servei licitat haurà de participar en la evolució d'aquest ecosistema de manera coordinada amb la resta d'equips que fan us de les solucions existents.

e) <u>Resposta prioritzada segons els requisits d'intel·ligència i nivell de criticitat.</u>

En cas que tingui lloc un nombre d'incidents simultanis que superi les capacitats de l'equip de resposta enfront d'incidents, cal definir una prioritat que s'establirà segons la criticitat dels actius implicats, la informació que es pot veure compromesa o l'alteració de l'operativa

de negoci que pot veure's afectada i el criteri del servei de Intel·ligencia operativa del CERT. De la mateixa manera s'ha de definir també quant esforç ha de ser invertit en la gestió d'un mateix incident i quan aquest s'ha de donar per finalitzat.

f) <u>Anàlisi forense de dispositius en entorns on premise, núvol i mòbils.</u>

En el cas que sigui necessari, arrel d'un potencial incident de seguretat s'ha d'obrir investigació amb la finalitat de poder determinar el què, qui, com i el per què de l'incident.

- La prestació del servei requereix d'una alta capacitat tècnica d'anàlisi forense, com a mínim, en les següents disciplines:
  - Network Forensics .
  - System Forensics (Windows / Linux&Unix / MacOSx / etc.).
  - Mobile Forensics.
  - Cloud.
  - OSINT.
- Anàlisi de la informació i les evidencies.

  Cal portar a terme l'anàlisi forense de les dades i les evidencies, utilitzant les eines aprovades per l'Agència, per les quals s'haurà de mantenir un registre actualitzat, segons grau d'actualització i llicenciament. Sempre que sigui possible l'anàlisi s'ha de realitzar sobre còpies clonades de les dades originals per tal de garantir la validesa de les mateixes.
- Registre dels resultats.

  Tota la informació associada als resultats de l'anàlisi forense de les evidències ha de quedar reflectida en un registre de resultats que ha de seguir una plantilla preestablerta (fitxa d'investigació / Informes de l'incident). Aquest registre ha de contenir totes les dades rellevants que puguin posar de manifest el tipus d'evidència tractada, la informació que aporta i les seves implicacions amb l'incident vinculat.
- Presentació dels resultats.

  La informació associada als resultats de l'anàlisi forense s'ha emmagatzemat en el registre de resultats disponible. Els resultats han de demostrar de manera clara i concisa la relació entre les evidències analitzades i les troballes identificades, per tal de generar un relat coherent que expliqui de manera entenedora la evolució de l'incident.

  Els resultats s'han de presentar de manera normalitzada, segons els procediments establerts a l'Agència i utilitzant estàndards internacionals.

  S'han d'obtenir unes conclusions que aportin un valor afegit, per tal de millorar la resposta enfront de l'incident associat a les evidències analitzades, i als posteriors incidents de caràcter similar que puguin tenir lloc.
- El servei ha de tenir la capacitat per defendre la seva conclusió davant una investigació realitzada, la seva conclusió de l'analítica i les seves conclusions.
- Es rellevant en aquest servei, el poder industrialitzar processos analítics repetitius, el que pot derivar en la necessitat de que aquest servei disposi de capacitat de desenvolupament d'eines (scripting, etc.). Aquest desenvolupament intern ha d'estar

autoritzat pels responsables del servei per part de l'Agència, i realitzar-se subjecte a la normativa interna de l'Agència.

g) <u>Desenvolupament de capacitats de resposta davant la evolució de les ciberamenaces</u>

S'ha d'assegurar que les capacitats d'investigació i anàlisi disponibles són adequades per tal de poder gestionar els principals incidents de ciberseguretat en tot moment, evolucionant-les quan sigui necessari per tal de garantir una gestió dels incidents que sigui efectiva i eficient.

h) <u>Anàlisi estàtic i dinàmic de mostres de malware.</u>

A més dels punts de l'apartat anterior, el servei ha de tenir capacitat per realitzar anàlisis de malware estàtic amb eines com IDA, Radare o Ghidra i anàlisi dinàmic manual o amb les diferents sandbox que disposa l'Agència, tant de codi obert com de diversos fabricants.

Aquesta anàlisi es pot fer amb les pròpies eines que disposa l'Agència en el seu laboratori, com en el laboratori de licitador o servei intern si disposa d'ell.

i) <u>Manteniment i evolució de la documentació i processos de resposta.</u>

Tota la informació associada a una actuació en enfront d'un incident ha de quedar reflectida en un registre de resultats que ha de seguir una plantilla preestablerta. Aquest registre ha de contenir com a mínim totes les dades rellevants que puguin posar de manifest el tipus d'incident que ha tinguin lloc, les accions dutes a terme, el resultat d'aquestes i l'estat en què ha quedat l'incident.

Durant el registre de resultats s'han de normalitzar els indicadors de compromís associats als incidents (IOC's), amb la finalitat de poder compartir la informació de manera normalitzada amb tercers si és necessari.

Tota la informació registrada ha de seguir estàndards de normalització com p.e *MITRE ATT&CK.*

La gestió dels patrons i IOC's d'un incident o grup d'incidents han de ser analitzats mitjançat la dinàmica TTP (Tactics, Techniques and Procedures) on s'han d'identificar els patrons d'activitat o mètodes utilitzats per un actor o grup d'actors per tal d'explotar un vector d'atac.

Els principals tipus d'incidents gestionats habitualment han de tenir els seus respectius playbooks associats i actualitzats.

j) <u>Suport en el compliment normatiu i les polítiques de resposta a incidents.</u>

El servei licitat ajudarà amb el seu coneixement i experiència a millorar el marc normatiu rellevant per l'Àmbit dins el marc de la ciberseguretat, així com a recomanar les millors polítiques de resposta a incidents. Juntament amb la resta de requeriments definits al present plec, s'ha de contribuir a millorar la preparació de l'Àmbit enfront incidents de ciberseguretat complexos.

Cal tenir en compte el mostrar la capacitat per a la gestió d'incidents de descrits anteriorment, automatització, tàctica de resposta i experiència en preparació per enfrontar-los (incident readiness).

3.2.3.2 Cerca proactiva d'incidents

La subfunció de cerca proactiva d'amenaces es centra en la identificació i l'anàlisi proactiu d'activitats sospitoses o malicioses abans que es produeixi un incident de seguretat. Aquest procés implica l'ús de tècniques d'anàlisi avançades, com l'exploració de xarxes, l'estudi de comportaments anòmals i la monitorització de possibles vulnerabilitats. L'objectiu és detectar amenaçes de manera preventiva, mitjançant l'ús de dades, intel·ligència i eines de monitorització, per tal de reduir el risc de danys i evitar o detectar incidents latents.

a) <u>Capacitat per a desenvolupar i executar freqüentment missions de cerca proactiva d'incidents</u>

- Execució de missions de "*Hunting"* de per tal de buscar intrusions o possibles intents d'intrusió en la infraestructura del client, així com l'explotació de vectors d'atac. Per dur a terme aquesta activitat s'han de valer, entre d'altres de:
  - Correlació avançada d'esdeveniment.
  - Detecció d'anomalies i canals encoberts.
  - Contextualització de la informació externa sobre ciberamenaces.
- **Capacitat d'anàlisi d'esdeveniments en els següents camps:**
  - Network Forensics .
  - System Forensics (Windows / Linux&Unix / MacOSx / etc.).
  - Mobile Forensics.
  - Cloud.
  - OSINT
- **El resultat d'aquesta recerca ha d'aportar com a mínim:**
  - La identificació de possibles incidents de ciberseguretat ja materialitzats a l'Àmbit.
  - La generació de noves regles de detecció, que es poden traduir en nous casos d'ús de SIEM, nous indicadors de compromís, etc.
  - La identificació de canvis que s'han d'aplicar a la configuració de la infraestructura per tal de garantir una millor capacitat de resposta davant d'incidents. P.ex. l'activació de l'auditoria d'un tipus de log específic o la extensió del període de retenció de certes traces.
  - La generació i adaptació de signatures de protecció del perímetre (Antivirus, IPS, Filtrat de Continguts, etc.).
  - Generació d'indicadors de compromís, considerant p. ex. adreces IP, dominis, adreces de correu electrònic, noms d'usuari i noms de fitxers sospitosos.

- La proposta d'implantació de noves eines i d'integració de noves fonts de traces.

❖ **Creació i revisió de casos d'ús per a alimentació del SOC.**

Es donarà suport a les altres equips per a la creació de casos d'us o implementació de regles i indicadors de compromís detectats mitjançant les missions de recerca realitzades o altres actuacions.

❖ **Desenvolupament de noves tècniques d'anàlisi**

Es realitzaran proves de concepte amb vulnerabilitats, eines o tècniques utilitzades per actors coneguts o detectades en incidents anteriors per al desenvolupament de noves capacitats com:

- Ampliació de l'abast de l'adquisició de dades per a anàlisi futurs
- Desenvolupament de regles específiques per a la detecció
- Creació de noves hipòtesis per a les activitats de recerca

❖ **Identificació de TTP (tàctiques, tècniques i procediments).**

S'analitzaran les tècniques, tàctiques i procediments utilitzades pels atacants així com la creació de noves hipòtesis per a les activitats de recerca, amb l'objectiu de millorar les diferents línies de defensa implementades als Àmbits d'actuació de l'Agència.

❖ **Contextualització i comprensió d'escenaris.**

S'analitzaran els diferents escenaris tant interns com externs, així com identificar-los a l'Àmbit per contextualitzar-los a l'entorn i veure quins són els aspectes centrats en un anàlisi de Risc vs Impacte.

❖ **Identificació d'amenaces desconegudes conjuntament amb la funció d'Intel·ligència Operativa.**

Es realitzaran anàlisi d'amenaces desconegudes als Àmbits d'actuació de l'Agència mitjançant tècniques de cerca i analítica de dades.

❖ **Identificació de millores i fine-tunnig d'eines.**

A totes les eines dintre de l'entorn que permetin la detecció proactiva d'incidents de ciberseguretat, es participarà en la millora de la configuració i correcta parametrització.

❖ **Establiment de contactes amb equips de seguretat locals en diferents països per identificar noves amenaces i desenvolupar nous mecanismes de detecció.**

❖ **Automatització de processos.**

Millora i industrialització en els processos de cerca proactiva d'incidents (identificació, cerca de casos d'ús/amenaces, IOC, etc.)

Cal tenir en compte el mostrar una metodologia, estratègia i planificació per a realitzar missions de cerca proactiva d'incidents (threat hunting).

3.2.3.3 Gestió d'evidències

La subfunció de gestió d'evidències és l'encarregada del tractament i conservació de les diferents evidències rebudes o generades arrel d'un incident de seguretat o d'una cerca proactiva, l'objectiu principal és garantir la seva integritat durant el cicle de vida d'aquestes, cobrint des de l'adquisició fins a la destrucció.

a) **Col·laboració en investigacions amb tercers garantint cadenes de custòdia**

- **Recepció de les evidències utilitzades**

  S'han de rebre les evidències utilitzades durant l'anàlisi forense, la recepció s'ha de dur a terme mitjançant mètodes segurs que mantinguin la cadena de custòdia en tot moment, com per exemple disc durs xifrats a nivell de hardware.

- **Categorització de les evidències**

  Un cop s'han rebut les evidències, aquestes han de ser categoritzades i etiquetades de forma inequívoca, per tal de poder ser emmagatzemades i, de ser necessari, recuperades per tal de ser utilitzades en un altre anàlisi o per ser utilitzades en processos judicials, per tant, aquesta categorització ha de mantenir la cadena de custòdia, i ha de seguir un estàndard com per exemples els proposats per SANS

- **Adquisició de tota la informació i evidències que es requereixin analitzar**

  La recol·lecció ha de seguir una planificació per tal de complir amb els estàndards internacionals d'anàlisi forense com SANS; ha de seguir els processos d'adquisició, anàlisi, custodia i destrucció de les evidències, i cal realitzar mitjançant eines que s'han d'adequar al manteniment de la cadena de custòdia, per tal de no afectar de cap manera la integritat de les dades i les evidències, ja que aquestes podran ser utilitzades en un procés legal/judicial.

- **Preservació de tota la informació i evidències adquirides**

  Totes les dades obtingudes durant la fase d'adquisició s'han d'emmagatzemar en un entorn especialment dissenyat i controlat per aquesta tasca, per tal de mantenir la cadena de custòdia. L'accés a aquest entorn de custòdia ha d'estar extremadament controlat i només sota ordes explícites del client o ordres de caràcter legal. El client designarà en cas que fos necessari, les condicions d'accés, per exemple, la presència d'un notari duran l'operació d'accés.

  Les evidències, un cop categoritzades, han de ser emmagatzemades i preservades de forma segura, per tal de mantenir la cadena de custòdia, tant en el moment de l'emmagatzematge com en el futur. El repositori d'evidències ha d'estar aïllat, i ha de limitar-se els punts d'accés i les credencials per tal que només les persones autoritzades puguin accedir-hi i deixar les evidencies.

- **Inventariat de les evidències**

  L'evidencies s'han d'inventariar per tal de tenir un control d'estat i vigència segons normativa de preservació establerta. Aquest inventariat ha de seguir una definició normalitzada i totes les evidències adscrites a l'inventari han de ser introduïdes segons aquesta.

- **Col·laboració amb tercers**

  La gestió d'evidències implica en certs casos haver de col·laborar amb tercers garantint en tot moment la cadena de custòdia. Aquests poden ser requeriments dels

Departaments per la política de la Generalitat de Catalunya, col·laboració amb forces i cossos de seguretat de l'estat en investigacions judicialitzades o similars.

3.2.3.4 Avaluació de las capacitats de resposta a incidents

La subfunció d'avaluació de les capacitats de resposta és l'encarregada de dur a terme les activitats necessàries que permetin a l'Agència avaluar l'estat de preparació enfront un incident de seguretat a les diferents entitats dins de l'àmbit d'actuació d'aquest contracte. A més ha de assegurar la preparació i formació de les entitats davant els incidents més habituals.

a) <u>Desenvolupar i dur a terme campanyes per a la preparació de les entitats</u>

- **Simulacres d'incidents**

Desenvolupament d'escenaris per a la realització de simulacres de manera anual, com a mínim, als 60 hospitals públics de Catalunya. Els simulacres han de donar a la entitat un seguit de directrius i han de permetre experimentar la presa de decisions crítiques en un context controlat per tal de assegurar una resposta efectiva en cas d'incident.

- **Exercicis d'avaluació de les capacitats de resposta**

Desenvolupament d'exercicis que permetin avaluar el grau de preparació de les diferents entitats segons les seves capacitats, com per exemple la capacitat de reiniciar contrasenyes de tots els usuaris, per bloquejar indicadors en el context d'un incident, etc. L'avaluació no és únicament tècnica sinó que s'avaluen els processos aplicats per resoldre cadascú d'aquests exercicis.

Aquest exercicis han de integrar-se dins dels simulacres per a la contextualització del mateixos i el enteniment per part de la entitat.

- **Avaluació del grau de traçabilitat per investigacions**

Les campanyes de preparació també han de servir per a avaluar l'estat de l'entitat davant una eventual recerca. En aquest sentit es mesuraran les capacitats de traçabilitat de les entitats per a detectar i mitigar possibles limitacions o faltes, així com per a millorar i establir mesures concretes que aportin un valor extra a les recerques futures**.**

- **Ampliació de la informació de context**

Tota la informació generada durant aquests exercicis ha de ser inclosa a la informació ja disponible, de tal manera que davant un incident de seguretat es pugui articular per donar una resposta més efectiva i a mida de l'entitat.

Cal tenir en compte el mostrar la seva experiència en metodologia, estratègia i planificació per a la gestió d'evidències.

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

Producte	Periodicitat
Informe executiu d'incident	Puntual
Presentació executiva d'incident	Puntual

Informe tècnic d'incident de ciberseguretat	Puntual
Presentació executiva cerca proactiva d'amenaces	Puntual
Informe tècnic de cerca proactiva d'amenaces	Puntual
Informe tècnic de Incident Readiness	Anual per entitat
Presentació de resultats per Incident Readiness	Anual per entitat
Desenvolupament presentació amb escenari per simulacres	Anual
Fitxes internes de seguiment d'incidents	Puntual
Fitxes execució de missions de recerca proactiva d'incidents	Puntual
Informe de mètriques i indicadors de Servei per àmbit amb el resultat del seu anàlisi.	Mensual
Informe resum dels incidents. Anàlisi d'estat de situació amb propostes de millora en curs, i problemàtiques associades.	Mensual
Informe d'anàlisi/problemàtica d'una tipologia determinada d'incident de seguretat, per exemple infeccions recurrents en un entorn, compromís reiteratiu d'una tipologia d'actiu, etc.	Puntual

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

3.2.3.1 Serveis no recurrents

Addicionalment als serveis recurrents descrits anteriorment, l'Agència també podria arribar a necessitar suport addicional en la Resposta a Incidents a l'àmbit 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:

- Gestió d'incidents
- Cerca proactiva d'amenaces
- Gestió d'evidències
- Avaluació de las capacitats de resposta

4 Condicions d'execució del servei

4.1 Horaris

El servei s'haurà de prestar d'acord amb els horaris de prestació dels serveis de l'Agència, 12x5 en horari de dies laborables. Es considera horari de dies laborables els dies que siguin laborables al centre de treball de l'Hospitalet de Llobregat amb prestació de 8:00h a 20:00h.

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

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

4.2 Localització física.

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

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

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.

4.3 Equip de treball

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

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

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.
- Habilitat per identificar, analitzar i resoldre problemes.
- Capacitat de treball sota pressió.
- Coneixement de català, castellà i d'anglès, parlat i escrit.
- Ampli coneixement legal, tecnològic i de negoci de seguretat informàtica i de l'entorn de l'administració pública.
- Altres necessaris per al bon desenvolupament dels serveis.

El licitador proposarà un equip de treball (descrivint-ne els perfils, dedicació, pla de treball, etc.) per a l'execució dels serveis sol·licitats en el present plec, d'acord amb les condicions i paràmetres esmentats en els apartats d'aquest plec.

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

4.3.1 Líder Tècnic

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

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

- Assegurament de la qualitat del servei prestat i dels lliurables generats (*Quality Assurance*).
- Gestió de riscos operatius del servei.

4.3.2 Expert en Avaluació de les Capacitats de Resposta

L'adjudicatari també, amb independència del model organitzatiu proposat, haurà de identificar el rol de **Expert en Avaluació de Capacitats de Resposta,** la activitat d'aquest rol és compatible amb les funcionalitats i característiques del perfil expert. Aquest rol és l'encarregat i responsable de la subfunció d'Avaluació de Capacitats de resposta a les entitats per tal de assegurar la capacitat recurrent per dur a terme les activitats incloses en aquesta. A més, ha d'assegurar que els següents punts s'executen dins d'aquest context:

- Dur a terme simulacres, com a mínim, amb els 60 hospitals públics de Catalunya, al menys una vegada a l'any
- Desenvolupament d'exercicis de simulacres segons les amenaces actuals que apliquin a l'àmbit d'actuació.
- Definició d'activitats i exercicis per a la mesura de les diferents capacitats de resposta dins de la entitat.
- Gestió punt a punt de la iniciativa. Des de la realització del simulacre, planificació de les sessions, anàlisi dels resultats i elaboració d'informes de resultats i estat.
- Reportar els resultats de les diferents capacitats que permetin a l'Agència determinar l'estat de preparació
- Mantenir, ampliar i articular la informació de context disponible a partir dels resultats generats.

4.3.3 Estructura

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

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

L'estimació aproximada d'hores efectives totals necessàries per l'execució dels serveis **recurrents** demanats en aquest plec és de **7.040 hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	Hores anuals mínimes
Expert d'incidents – 2 FTE al 100% de dedicació-	**3520 hores**
Tècnic de Resposta a Incidents	**3.520 hores**

Així mateix, dins d'aquestes **7040 hores** es contempla la necessitat d'una dedicació mínima a la evolució del servei i el seu ecosistema. S'estima el següent número d'hores mínimes anuals per aquestes tasques (assumibles per qualsevol dels perfils mínims).

Concepte	Hores anuals mínimes
Evolució	**1760 hores**

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

4.3.4 Perfils

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

Perfil	Requisits
Expert d'incidents	• 5 anys d'experiència demostrable en el món de la seguretat. • 3 anys d'experiència demostrable en gestionar Equips tècnics de Resposta enfront d'Incidents. • 3 anys d'experiència en la gestió i lideratge enfront d'Incidents crítics. • Coneixements avançats de la majoria de sistemes operatius, xarxes, bases de dades, softwares de control, softwares de treball, softwares de seguretat perimetral i monitoratge entre d'altres, en especials els utilitzats pel client. • Capacitat proactiva per analitzar i definir línies de resposta enfront d'incidents. • Coneixements avançats d'anàlisi forense. • Coneixement en gestió de cadena de custòdia i evidències. • Coneixement de la legislació i normatives vigents en l'àmbit de la gestió d'incidents. • Capacitat proactiva, resolutiva i dots de lideratge.
Tècnic de Resposta i recerca proactiva d'incidents	• 3 anys o més d'experiència demostrable en el món de la seguretat. • Coneixements en resposta enfront d'incidents. • Coneixements avançats sobre 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. • Coneixements en eines de control perimetral i monitoratge, especialment aquelles que utilitza el client. • Coneixements en gestió de cadena de custòdia. • Coneixements de la majoria de sistemes operatius, xarxes, bases de dades, softwares de control, softwares de treball, softwares de seguretat perimetral i monitoratge entre d'altres. • Capacitat proactiva i resolutiva.

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.

4.4 Canvi de recurs

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

4.5 Control de rotació

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

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

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

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

4.6 Eines i equipament per a la prestació de serveis.

Les principals eines requerides (gestió d'esdeveniments, alertes, sistema de registre, anàlisi de codi, web i infraestructura...) per la prestació del servei seran proporcionades per l'Agència. 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.

- Correu electrònics i eines ofimàtiques i col·laboratives Suite O365.
- Ordinadors de laboratori per ús del proveïdor i/o sistemes i entorns d'anàlisi i proves per dur a terme tasques pròpies de la funció com per exemple.....

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.

4.7 Gestió del coneixement

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

4.8 Seguretat Corporativa

Un cop adjudicat el contracte basat, tant l'empresa adjudicatària com el personal de l'empresa adjudicatària s'haurà de sotmetre a les polítiques i regulacions internes que estableix l'àrea de Seguretat Corporativa en matèria de seguretat de la informació:

- 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.
- 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.

4.9 Control de Gestió

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

- De complir amb el model de seguiment econòmic i planificació en termes de capacitat i execució de tasques.
- D'ajustar-se als procediments de facturació que determini l'Agència.
- De conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència, d'acord amb els procediments establerts.
- D'exercir la gestió del contracte amb capacitats de *forecast.*
- Realitzar el *reporting* en les eines proporcionades per l'Agència amb els següents conceptes.

- Fitxer mestre de persones.
- Fitxer mestre de projectes i activitats.
- Estimació de recursos per projecte.
- Seguiment dels riscos.
- Seguiment del consum de recursos.
- Imputació de temps i activitats.
- Assignació de tasques a persones.
- Memòria d'activitat del contracte.
- Facturació i Conformació de factures.

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

4.10 Documentació.

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

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

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

4.11 Formació

El personal de l'empresa adjudicatària del contracte basat realitzarà, si s'escau, formació continuada per tal de garantir l'actualització dels seus coneixements així com l'adquisició de nou coneixement que pugui ser de valor pels serveis de l'Agència.

4.12 Contingència

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

- Estacions de treball amb el programari adequat per realitzar les tasques descrites.
- Comunicacions d'accés a les aplicacions informàtiques.

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

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

4.13 Metodologia, estàndards i lliurables

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

4.14 Seguretat

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

3.11.1. 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.

3.11.2. Dades de caràcter personal

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

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

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

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

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

3.11.4. Capacitat tècnica

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

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

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

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

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

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

Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centre Criptològic Nacional o, en el seu defecte, acreditar que el producte o servei disposa de requeriments equivalents.

3.11.6. Interconnexions

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

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

3.11.7. Verificació del compliment i auditoria

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

3.11.8. Incidents de seguretat

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

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

3.11.9. Accés a la informació

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

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

3.12. 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.

3.13. Seguiment del servei

Les empreses adjudicatària haurà de presentar un informe de seguiment. 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.

3.14. 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.