Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya

Contractació del Servei de Suport al Catalonia CERT CO.04.2021

Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya

Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya

ÍNDEX

1 INTRODUCCIÓ 1

1.1 OBJECTIUS ESTRATÈGICS 1
1.2 L'AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA 1
1.3 SOC/CERT 2
1.4 CONTEXT DELS SERVEIS 2

2 LOT 1: SERVEI DE SUPORT DE RESPOSTA ACTIVA 11

2.1 OBJECTE DE LA LICITACIÓ 12
2.2 ORIENTACIÓ 12
2.3 DESCRIPCIÓ 13
2.4 OBJECTIUS DEL SERVEI 13
2.5 REQUISITS DEL SERVEI 14
2.6 GESTIÓ DEL SERVEI 22
2.7 ROLS I FUNCIONS 23
2.8 VOLUMETRIES ACTUALS 24
2.9 LLIURABLES DEL SERVEI 24
2.10 MILLORA DELS SERVEIS 26

3 LOT 2: SERVEI DE SUPORT D'INTEL·LIGÈNCIA OPERATIVA 27

3.1 OBJECTE DE LA LICITACIÓ 28
3.2 ORIENTACIÓ 28
3.3 DESCRIPCIÓ 29
3.4 OBJECTIUS DEL SERVEI 29
3.5 REQUISITS DEL SERVEI 31
3.6 GESTIÓ DEL SERVEI 37
3.7 ROLS I FUNCIONS 38
3.8 VOLUMETRIES ACTUALS 38
3.9 LLIURABLES DEL SERVEI 40
3.10 MILLORA DELS SERVEIS 41

4 CONDICIONS D'EXECUCIÓ 43

4.1 HORARI DEL SERVEI 43
4.2 UBICACIÓ FÍSICA 43
4.3 EQUIPS DE TREBALL 44
4.4 PERFILS 46
4.5 IDIOMA DEL SERVEI 47
4.6 EINES 47
4.7 GOVERN DE LA DADA I GOVERN DEL RISC 48
4.8 INFRAESTRUCTURA I EQUIPAMENT PER LA PRESTACIÓ DELS SERVEIS 49
4.9 SEGURETAT CORPORATIVA 50
4.10 CONTROL DE GESTIÓ 51
4.11 PROPIETAT I VALIDACIÓ DE LA DOCUMENTACIÓ 52
4.12 INTEGRACIÓ AMB ALTRES EQUIPS 52
4.13 INNOVACIÓ 54

5 ACORDS DE NIVELL DE SERVEI I PENALITZACIONS 54

5.1 MODEL DE MESURA DEL NIVELL DE SERVEI 55
5.2 MODEL DE PENALITZACIONS 59

6 FASES DE LA PRESTACIÓ 62

6.1 TRANSICIÓ 62
6.2 NOVA PRESTACIÓ 63
6.3 DEVOLUCIÓ 63

7 ANNEX I – LLISTAT D'EINES 65

8 MARC NORMATIU 66

1 INTRODUCCIÓ

1.1 OBJECTIUS ESTRATÈGICS

L'Agència de Ciberseguretat de Catalunya (en endavant, l'Agència), té la necessitat de licitar el present contracte per a l'execució de les funcions de seguretat TIC en virtut de l'"Acord del Govern pel qual s'aprova el contracte programa entre l'Administració de la Generalitat de Catalunya, mitjançant el Departament de Polítiques Digitals i Administració Pública, i la Fundació Centre de Seguretat de la Informació de Catalunya per als anys 2019-2022, de 5 de Febrer de 2019."

L'Agència, amb aquest encàrrec del Govern, assumeix funcions i responsabilitats en l'àmbit de la ciberseguretat, esdevenint així una peça cabdal en l'estratègia de ciberseguretat del Govern de Catalunya.

Com a part d'aquesta estratègia, i en consonància amb les necessitats de les diferents entitats públiques a qui presta servei, l'Agència necessita dotar-se de les millors pràctiques, eines i proveïdors, per portar a terme els seus serveis.

1.2 L'AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

L'Agència és l'ens públic que succeeix la Fundació Centre de Seguretat la Informació de Catalunya (CESICAT), que va néixer l'any 2010, arran de l'acord de govern GOV/50/2009 del 17 de març i l'autorització de constitució de la Fundació Centre de Seguretat de la Informació de Catalunya.

Així, l'Agència de Ciberseguretat de Catalunya se subroga en els convenis i contractes subscrits de la Fundació Centre de Seguretat de la Informació de Catalunya a data 1 de gener de 2020 en virtut d'allò que estableix la disposició addicional segona de la Llei 15/2017, del 25 de juliol, de l'Agència de Ciberseguretat de Catalunya, així com el Decret 223/2019, de 29 d'octubre, pel qual s'aproven els Estatuts de l'Agència de Ciberseguretat de Catalunya, els béns i actius que s'adscriuen a l'Agència, així com els drets i obligacions a què l'Agència se subroga.

La seva finalitat és garantir una Societat de la Informació segura al conjunt de la societat catalana i de la seva Administració Pública, amb voluntat d'esdevenir un referent a nivell nacional i internacional en matèria de ciberseguretat, i que té el patrimoni, els rendiments i els recursos dedicats a la realització de les finalitats d'interès general previstes en els seus estatuts.

Avui en dia, la tecnologia es presenta com un element transversal i inherent a l'activitat humana tant personal, social, professional, com institucional, essent doncs un repte i una obligació per a l'Administració el fet de treballar i garantir la seguretat tecnològica a la ciutadania en tot el seu àmbit. Conscient de la importància creixent i la necessitat de vetllar per la seguretat en els sistemes de la informació, i en especial de les identitats que gestionen aquesta informació, l'Agència ha definit un model de seguretat de la informació, per tal de ser desplegat de manera homogènia i extensible a tota l'Administració Pública catalana, començant per la Generalitat de Catalunya i el seu Sector Públic.

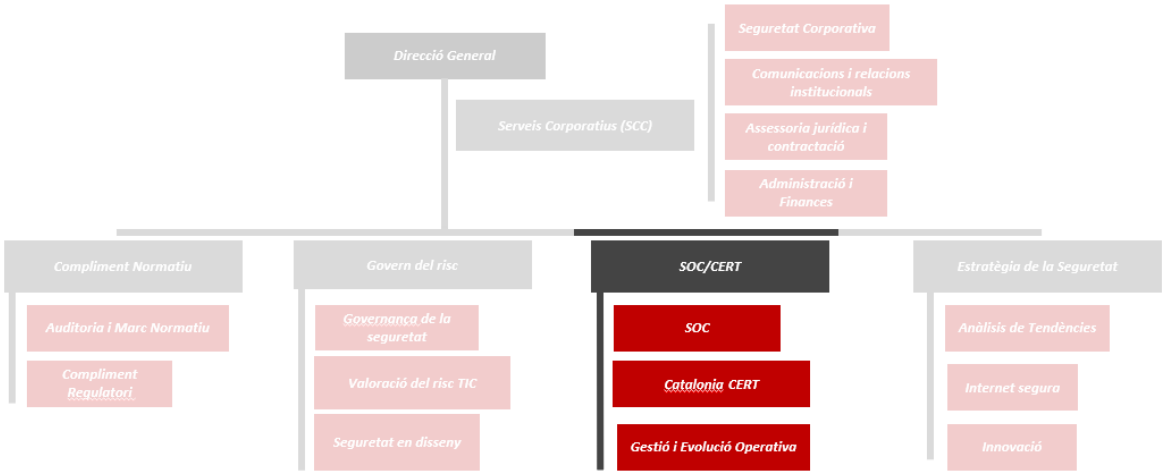
Els temps avancen i la digitalització social i de l'Administració dóna lloc i obliga a posar en valor aquest servei clau per a la societat i per a la pròpia Administració. El concepte i servei de la ciberseguretat esdevé un servei crític i bàsic cap a la ciutadania i un valor estratègic de país.

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

És per això que l'Agència té l'encomana de la planificació, gestió i control de la seguretat de les TIC de l'Administració de la Generalitat i el seu sector públic, duent a terme les mesures necessàries per assolir aquestes funcions.

1.3 SOC/CERT

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



Organigrama Agència de Ciberseguretat de Catalunya

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

- SOC (de "*Security Operations Center"* en anglès)
- Catalonia CERT
- Gestió i Evolució Operativa

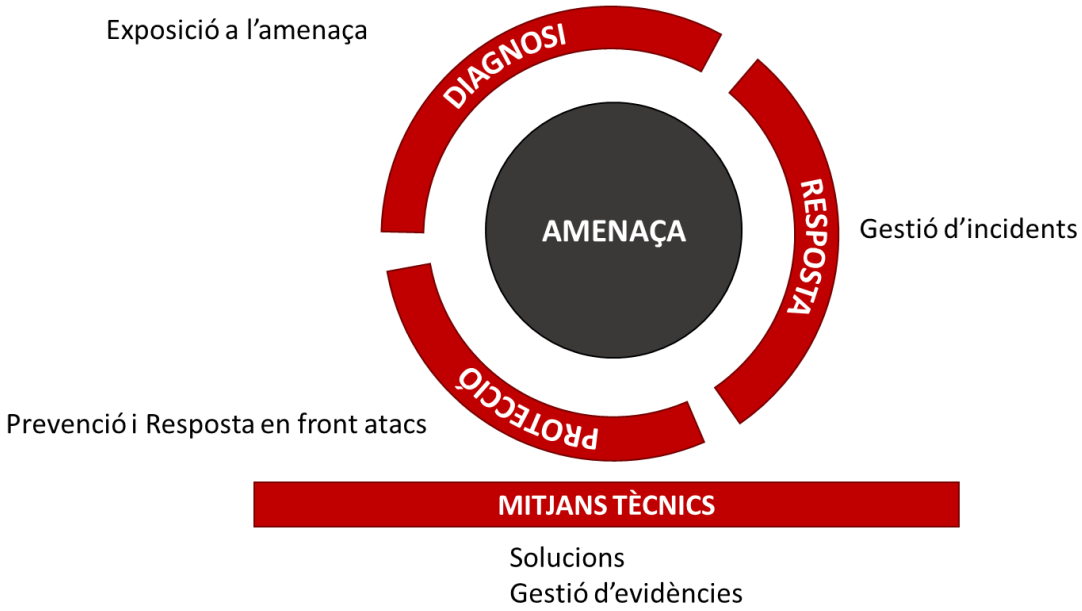
1.4 CONTEXT DELS SERVEIS

Els serveis objecte de la present licitació tenen com a objectiu fonamental donar suport a part del desenvolupament de les funcions i responsabilitats operatives que l'Agència de Ciberseguretat té assignades segons els marc legal i els successius encàrrecs, acords de Govern, acords de col·laboració i encàrrecs de Govern que ha rebut. L'objecte de la present licitació té per objectius principals contribuir a la prevenció, detecció, protecció i resposta davant d'esdeveniments maliciosos, ciberatacs i incidents de seguretat que puguin afectar a l'abast d'actuació de l'Agència de Ciberseguretat.

1.4.1 Catàleg de serveis

Per fer front a les necessitats que es deriven de la execució del Pla Estratègic i del compliment de les funcions assignades, es desenvolupa i manté un Catàleg de Serveis que articula la prestació de l'activitat de la entitat amb els diferents clients.

Actualment, el Catàleg de Serveis de l'Agència de Ciberseguretat conté entre d'altres els següents serveis que lidera l'àrea operativa de l'Agència de Ciberseguretat i que es detallen en aquest mateix document, fent èmfasi especial en l'objecte dels serveis licitats. Donat que el Catàleg de Serveis és l'eina fonamental per la comunicació amb els clients i el canal per a la oferta de serveis de l'Agència de Ciberseguretat als seus clients, la seva estructura i continguts podran canviar amb el temps i durant el període d'execució del servei que es licita.



Catàleg de serveis del SOC/CERT

Els principals serveis operatius disponibles des del SOC/CERT son els següents:

- **Exposició a l'amenaça**

  S'ofereix un anàlisi del comportament de les ciberamenaces actualment actives, fent focus en aquelles més rellevants, què es preveu poden afectar a l'àmbit, incloent detalls sobre la seva naturalesa i aportant les eines necessàries per poder prevenir-les, tant a nivell tècnic, com operacional, tàctic i, fins i tot, estratègic. A més, s'aporta una previsió del comportament d'aquestes amenaces, per poder justificar la presa de decisions i possibilitar la adequació dels plans de resposta de manera anticipada.

  Així mateix també proveeix un anàlisi de la superfície d'exposició d'un determinat àmbit, per tal d'identificar quines de les amenaces detectades podrien generar una afectació a l'àmbit amb més probabilitat. El resultat de l'anàlisi permet realitzar una priorització de les tasques de prevenció adients i justifica l'aplicació de les contramesures corresponents.

- **Gestió d'incidents**

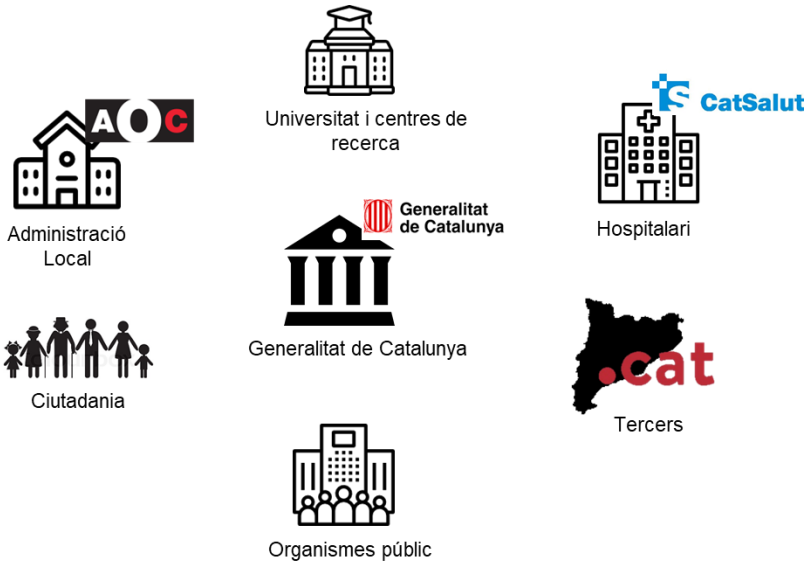
  Persegueix la identificació, contingència, erradicació i resolució eficient dels incidents de ciberseguretat que es produeixen a l'àmbit, minimitzant el seu impacte i contribuint a fer que el mateix tipus d'incident no es torni a repetir.

- **Prevenció i Resposta en front atacs**

  Permet evitar la materialització de les ciberamenaces mitjançant la resposta en front atacs i la reducció del grau d'exposició. Per habilitar de manera recurrent aquest servei i les capacitats associades de prevenció i resposta, es requereix el desplegament del principal producte de seguretat del SOC/CERT, el perímetre de seguretat.

1.4.2 Àmbits d'actuació

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



Àmbits d'actuació de l'Agència de Ciberseguretat de Catalunya

Els serveis de suport inclosos en aquesta licitació han de satisfer necessàriament les necessitats definides en el present document a tots 7 àmbits d'actuació:

- La Generalitat de Catalunya.
- L'Administració Local.
- Universitats i centres de recerca.

- Àmbit hospitalari.
- Organismes públics.
- Ciutadania.
- Tercers.

Els detalls inclosos als següents apartats sobre els àmbits d'actuació, juntament amb algunes de les volumetries reflectides, s'han d'entendre sempre com una estimació i ha de ser el propi servei licitat el responsable de, en col·laboració amb l'equip de *"Gestió Operativa"* del SOC/CERT, completar i ajustar l'abast per cada àmbit d'acord a la informació disponible en cada moment.

S'ha de tenir en compte també que es possible que, tot i que els àmbits definits son prou independents i el nivell de solapament entre ells hauria de ser residual, es dona la circumstància puntual de que algun actiu es pot catalogar dins de més d'un àmbit d'actuació simultàniament. Aquesta es una situació normal i el servei haurà d'adaptar-se de manera natural a aquesta circumstància.

1.4.2.1 Generalitat de Catalunya

Dins l'àmbit de la Generalitat de Catalunya, es defineixen uns actius prioritaris, nomenats SIC (Sistema d'informació Crític) i VIP (per les sigles en anglès de "*very important person*") en els quals l'Agència de Ciberseguretat de Catalunya ha de garantir especialment la seva seguretat.

Cal tenir en compte que l'Agència de Ciberseguretat de Catalunya, per tal de realitzar algunes de les funcions i responsabilitats operatives que li han sigut assignades cal relacionar amb altres entitats públiques, una de les més significatives és el CTTI (Centre de Telecomunicacions i Tecnologies de la Informació). Aquesta relació tan estreta amb el CTTI ve originada pel fet que és aquesta entitat qui gestiona els serveis TIC de la Generalitat de Catalunya externalitzats als diferents proveïdors que formen part del model TIC (desenvolupament, hosting/cloud, comunicacions i lloc de treball). Tenint això en compte, caldrà que el licitador sigui capaç d'executar els mecanismes adients per tal de fer la integració operativa amb els processos del CTTI (p. ex. obtenció d'informació, resolució d'incidents de ciberseguretat,...), així com canalitzar les comunicacions necessàries per a les vies i eines establertes internament.

Des de l'Agència de Ciberseguretat, els Responsables de Seguretat de la Informació (RSI) són els responsables d'aquest desplegament, de la demanda dels serveis que es deriva, de la relació amb el client i del lliurament final del servei cap al client. En aquests rol de gestors de la demanda, la prestació dels serveis aquí descrits proveeixen de les eines i dels mecanismes per portar a terme aquest objectiu cabdal del desplegament del model operatiu.

Igual que els RSI assumeixen, entre d'altres, aquest rol i funcions, els Responsables de la Línia de Servei (RLS), són les persones de l'Agència de Ciberseguretat que gestionen la capacitat, planificació i execució dels serveis demanats pels RSI i d'altres clients de l'Agència de Ciberseguretat. Els serveis que es descriuen en aquest plec, tenen, com a objectiu fonamental, donar el suport en l'execució d'aquests serveis.

Modelització de la gestió de la Ciberseguretat de la Generalitat de Catalunya.

Degut al model de gestió de les TIC a la Generalitat de Catalunya, amb una alta externalització dels mateixos, el model de gestió de la ciberseguretat de l'Agència de Ciberseguretat s'ha adaptat al mateix, tenint en compte les particularitats inherents a tot

model externalitzat, així com al seu govern per part del CTTI, òrgan encarregat de la gestió TIC de la Generalitat.

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

- El negoci de la Generalitat i propi dels seus Departaments.
- El model de gestió TIC externalitzat i dinàmicament canviant.
- Els serveis i objectius de ciberseguretat propis de l'Agència de Ciberseguretat.
- El model operatiu de la ciberseguretat.

1.4.2.2 Administració Local

Aquest àmbit d'actuació es cobreix els següents principals tipus d'entitats rellevants:

- Ajuntaments.
- Diputacions.
- Consells comarcals.
- Consorci AOC i d'altres.

1.4.2.3 Universitats i centres de recerca

L'àmbit de les universitats i els centres de recerca inclou, al menys:

- Universitats públiques.
- Instituts universitaris d'investigació.
- Facultats i escoles universitàries.
- Centres d'investigació.

1.4.2.4 Hospitalari

Aquest àmbit inclou al menys tots els hospitals arreu del territori i els organismes que els gestionen:

- Hospitals.
- Consorcis.
- Gerències territorials.

1.4.2.5 Organismes públics

Aquest àmbit inclou, en major o menor mesura, les entitats del sector públic de la Generalitat arreu del territori:

- Entitats del sector públic de la Generalitat.

1.4.2.6 Ciutadania

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

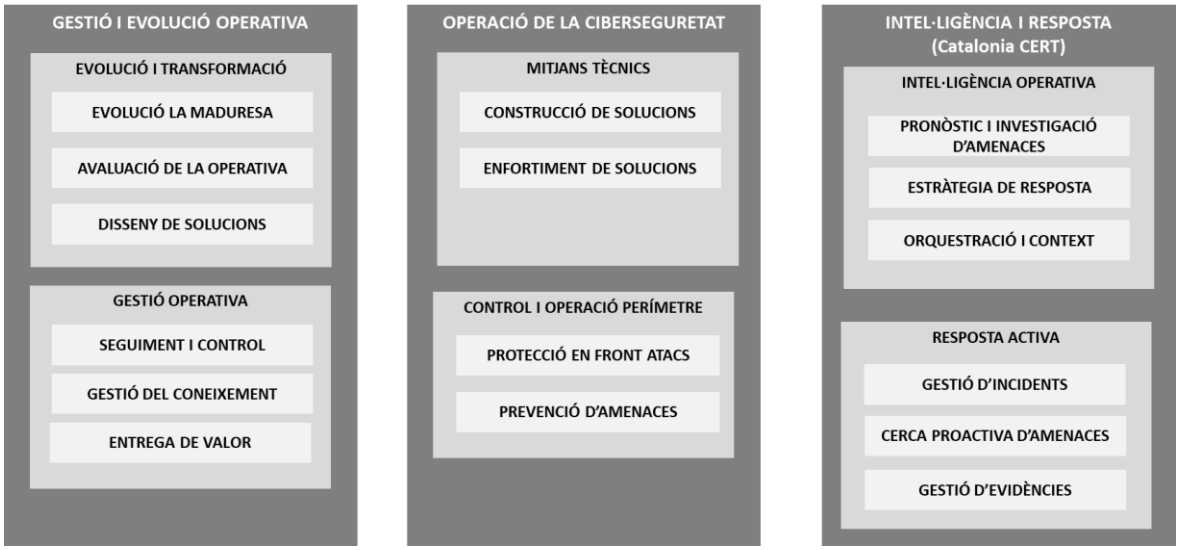
1.4.2.7 Tercers

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

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

1.4.1 Funcions del SOC/CERT

La següent figura mostra les 3 principals línies de treball que defineixen el SOC/CERT i reflecteix els diferents equips existents dins del SOC/CERT. Els serveis adjudicats es relacionaran amb aquestes altres funcions i amb els seus corresponents serveis de suport subjacents.



Funcions i subfuncions del SOC/CERT

El serveis inclosos en aquesta licitació han de complir amb totes les necessitats operatives de les funcions a les que donen suport, que es descriuen en aquest document i també **han**

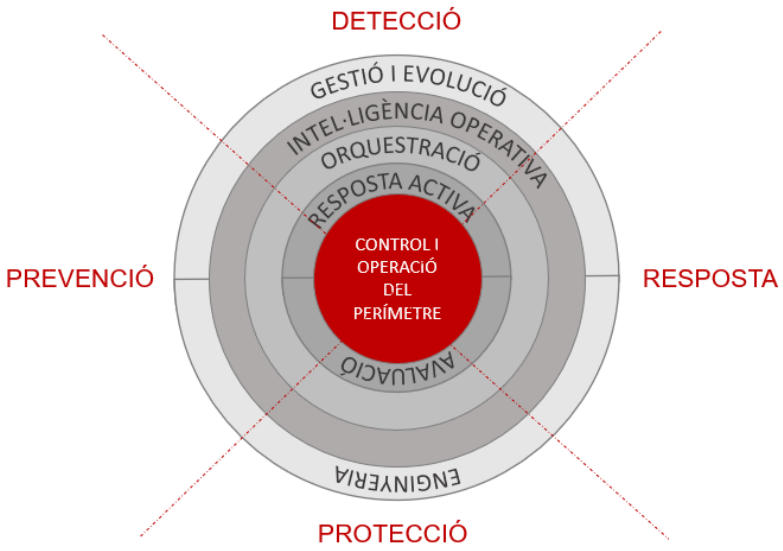
de donar suport a les necessitats de caràcter més tàctic i estratègic, que en aquest cas son assumides en major part pel personal de la pròpia Agència de Ciberseguretat.

S'espera dels licitadors d'aquests serveis que presentin detalladament les seves propostes de model, organització, metodologia, recursos i funcions que compleixin amb els requisits i cobreixin les necessitats de l'Agència de Ciberseguretat expressades en aquest plec, valorant-se específicament l'aportació de valor del licitador en forma de criteris, experiència, capacitats i coneixements per a assolir aquests objectius.

Com a Agència de Ciberseguretat de Catalunya, es valorarà l'experiència i capacitació en seguretat de la informació dels licitadors. De manera conseqüent, un requisit indispensable serà la consideració del vessant de la seguretat de la informació en tota activitat que es reculli en les propostes presentades.

1.4.2 Model funcional agregat

L'estructura funcional dins del SOC/CERT, juntament amb els serveis de suport a l'operació de l'Agència de Ciberseguretat de Catalunya sobre la que es sustenta, pretenen satisfer els quatre eixos fonamentals de la seguretat de la informació enfront d'amenaces i incidents de seguretat: detecció, prevenció, protecció i resposta. La distribució en funcions (amb els seus serveis de suport subjacents) té com a objectiu principal garantir la seguretat dels actius TIC de tot l'àmbit alhora que s'incrementa el nivell de maduresa actual de l'àrea d'operacions de l'Agència de Ciberseguretat de Catalunya.



Intel·ligència Operativa dins de l'estructura funcional del SOC/CERT

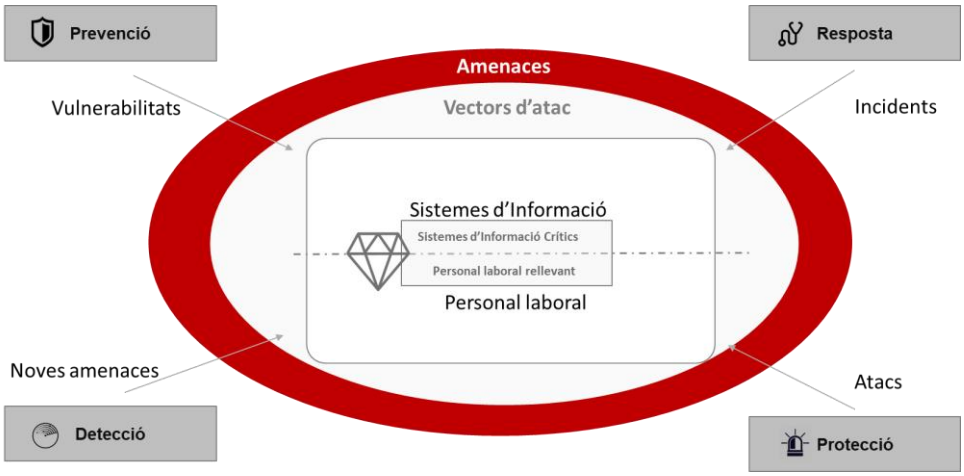
La funció de **Control i Operació del Perímetre (COP)** dona resposta a la operació de perímetres de la part de detecció prevenció i resposta . Aquest eix correspon a tasques relatives a la gestió del cicle de vida dels esdeveniments, vulnerabilitats, amenaces i atacs de ciberseguretat fins que aquests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

La funció **d'Avaluació Operativa (AOP)** dona suport a la resta de funcions, validant de manera colaborativa el seu criteri respecte als quatre eixos de detecció, prevenció, protecció i resposta.

Tot i la efectivitat dels controls i les tasques de prevenció desplegades, encara existeix la possibilitat de que una amenaça es materialitzi en un incident de ciberseguretat. Aleshores, la funció de **Resposta Activa (RAC)** s'activa de manera reactiva quan es detecta un incident de severitat elevada, per permetre reduir en temps i forma la seva afectació dins de l'àmbit i per garantir que el mateix tipus d'incident no torna a succeir en les mateixes circumstàncies.

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

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

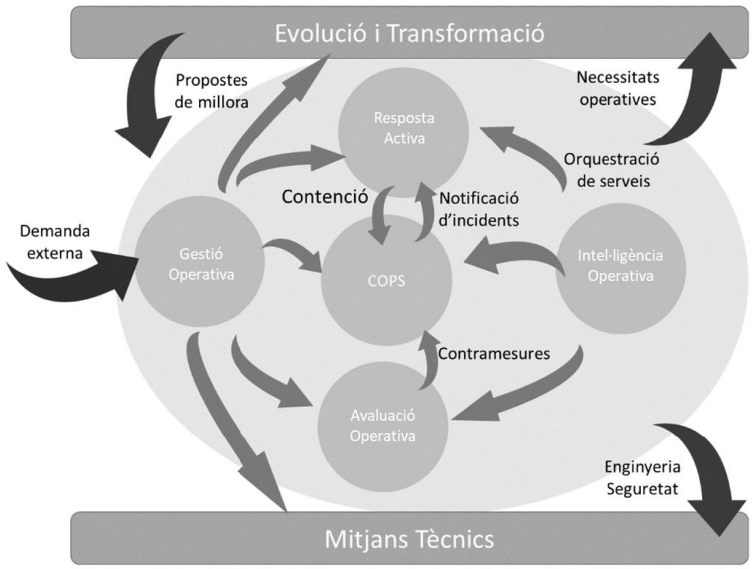


Plantejament "Threat-Centric"

Justament per sobre de l'Orquestració Operativa, es desplega la funció **d'Intel·ligència Operativa (IOP)**, que complementa l'activitat de les funcions anteriors, amb una visió orientada a l'anàlisi del context de la ciberseguretat de l'organització i l'àmbit d'actuació de l'Agència de Ciberseguretat. A partir de la informació resultant de l'operativa de les diferents funcions i els seus serveis de suport, d'altres entitats de l'àmbit de la ciberseguretat i de fonts externes de coneixement, es realitza una correlació i anàlisi en profunditat per tal de determinar patrons d'actuació i potencials noves ciberamenaces. Aquestes tasques s'associen a totes les fases de la Cyber Kill Chain del MITRE i també es realitza una tasca analítica de la operativa resultant de la resta de funcions.

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

Per últim i de manera transversal, la funció de Gestió i Evolució Operativa i la de Mitjans Tècnics contribueixen a la viabilitat de la resta de funcions: **Gestió i Evolució Operativa (GEO)** permet resoldre activament les necessitats i els problemes de les altres funcions del SOC/CERT, per garantir la gestió eficaç i eficient de les ciberamenaces, mentre que **Mitjans Tècnics (MTC)** principalment aporta i garanteix la disponibilitat de les soluciones tecnològiques que donen resposta a les necessitats de tota l'Agència de Ciberseguretat de Catalunya.



Exemplificació del model operatiu entre els diferents serveis.

Totes les funcions han de tenir en compte les accions i tasques necessàries per a gestionar les alertes que es reben respecte dels esdeveniments identificats amb les eines de seguretat de l'Agència de Ciberseguretat, tenint en compte tot el cicle de vida dels atacs, fins que són considerats incidents, sempre segons les fases definides a la Cyber Kill Chain de MITRE.

Kill-Chain segons MITRE ATT&CK

1.4.3 Estructura de Lots

Dins del context descrit al present apartat, es defineixen dos lots, que permeten donar suport a les dos funcions principals del Catalonia CERT:

- **Lot 1**: El servei principal de suport per a la funció de **Resposta Activa**, encarregada de gestionar incidents de ciberseguretat greus, reduint en temps i forma la seva afectació dins de l'àmbit i garantint que el mateix tipus d'incident no torna a succeir en les mateixes circumstàncies.
- **Lot 2** : Servei de suport per a la funció **d'Intel·ligència Operativa**, responsable d'aportar als àmbits d'actuació el coneixement i els plans d'actuació necessaris per permetre reduir, efectiva i eficientment, l'afectació de les ciberamenaces.

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

2 LOT 1: SERVEI DE SUPORT DE RESPOSTA ACTIVA

L'objectiu principal de la funció de Resposta Activa és reduir en temps i forma l'afectació enfront un incident, garantint que aquet no torni a succeir. Per tal de fer front a aquesta encomana, des del servei de suport licitat al Lot 1, es defineixen les funcions principals i les tasques mínimes que es consideren necessàries per a la correcta prestació dels serveis dins l'àmbit de resposta, tot i que no es pretén realitzar un llistat exhaustiu i serà el licitador qui haurà de proposar les funcions que realitzarà durant la prestació del servei tot tenint en compte les línies principals detallades en aquesta licitació.

Tot i les tasques de prevenció, detecció i protecció que es realitzen des de SOC (Security Operations Center), l'Agència de Ciberseguretat té un paper fonamental en les tasques de resposta a incidents de seguretat, aquest és precisament l'objectiu del servei de Gestió d'Incidents de Seguretat (GIS) dins de la funció de Resposta Activa.

Un incident s'entén com la materialització d'una ciberamenaça, atac dirigit als actius en l'àmbit d'actuació de l'Agència de Ciberseguretat que ha produït impacte, afectació dels serveis TIC, actius, sistemes d'informació, i/o de la informació que s'hi gestiona.

L'àmbit de Resposta, és el responsable del desenvolupament de les mesures preventives i reactives enfront d'incidents de seguretat TIC, responsable d'analitzar i proporcionar el servei reactiu necessari envers l'afectat i el seu context d'incidència, coordinació operativa, gestió de crisi, i portar a terme la investigació corresponent en cas que sigui necessària per a determinar l'abast de l'afectació, què, qui, quan, com i el per què d'aquest, que permeti determinar el succeït, i les accions a dur a terme per a què no es torni a reproduir.

La resposta davant d'un Incident de seguretat té en compte tot el cicle de vida d'aquest, des del la seva gestió, investigació i accions que s'hi derivin com pot ser la gestió de l'evidència, compartició d'indicadors, participació en plans d'evolució i millora, capacitació, identificació i seguiment d'incompliments normatius, com l'aplicació de la legislació vigent, atès l'objectiu final dins l'àmbit i de la mateixa Agència de Ciberseguretat, que no es produeixi cap incident de seguretat TIC.

La Resposta Activa a incidents permet a l'Agència de Ciberseguretat:

- Ajudar al públic objectiu (contingència) a mitigar i prevenir incidents greus de seguretat.
- Ajudar a protegir la informació.

- Coordinar de forma centralitzada la seguretat de la informació.
- Emmagatzemar i custodiar evidències, per si calgués al seu ús en un àmbit legal.
- Donar suport i prestar assistència a usuaris per recuperar-se de les conseqüències dels incidents de seguretat.
- Dirigir de forma centralitzada la resposta a incidents de seguretat, promoure la confiança, gestió de l'afectat.
- Participació i coordinació activa amb altres CERTs/CSIRTs, equips de resposta per tal d'acomplir amb les funcions encomanades.
- Ajuda a difondre la cultura de seguretat informàtica i crear mitjans de difusió per a organitzacions i individus.

Cal destacar que l'Agència de Ciberseguretat actualment disposa d'un laboratori de seguretat en el que es poden explotar eines amb l'objectiu de facilitar les tasques relatives al servei en qüestió, de les següents tipologies:

- Adquisició d'evidències i anàlisi forense.
- Anàlisi d'artefactes i codi maliciós.
- Estudi de contramesures i anàlisi de tràfic.
- Investigació d'actors i tècniques OSINT.

2.1 OBJECTE DE LA LICITACIÓ

El servei licitat inclou les tasques de suport a la funció de Resposta Activa i les seves subfuncions, que han de permetre l'assoliment de tots els objectius definits per l'Agència de Ciberseguretat de Catalunya.

2.2 ORIENTACIÓ

El licitador haurà de contemplar els següents principis que son els que regeixen el disseny del present servei de suport i la seva licitació:

- El servei **focalitzará** la seva capacitat en els **incidents que són de valor.** La resta seran governats però la seva gestió recau sobre proveidors dels diferents àmbits d'actuació de la l'Agència de Ciberseguretat.
- En aquesta línia, el servei ha de **garantir que els àmbits** estan contínuament **preparats** per poder dur a terme la resposta a incidents.
- 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 donar suport a l'Agència de Ciberseguretat de Catalunya en el **posicionament internacional** del Catalonia CERT, com a referent de ciberseguretat.

2.3 DESCRIPCIÓ

El servei de suport de Resposta Activa porta a terme la gestió complerta davant la materialització de les ciberamenaces, la gestió dels incidents de seguretat, investigació, anàlisi forense, i execució dels processos que s'hi puguin derivar com pot ser la identificació millores tecnològiques perquè aquests no tornin a succeir, processos o incompliments normatius.

Addicionalment, el servei de Gestió d'Incidents 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 de Resposta Activa són les següents:

- Gestió d'incidents
- Cerca proactiva d'incidents
- Gestió d'evidències

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

2.4 OBJECTIUS DEL SERVEI

El present apartat inclou un llistat d'objectius 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.

- **Reduir anualment els 5 principals tipus d'incident en cadascun dels àmbits d'acutació** millorant l'eficàcia, eficiència i satisfacció.
- **Millorar anualment els temps de resposta** pels **5 principals tipus d'incident** per cadascun dels **àmbits d'actuació**.
- Evolucionar l'infraestructura per donar resposta als incidents amb **un pla de revisió anual.**
- Revisar i actualitzar **un cop a l'any el compliment normatiu i polítiques de resposta** a incidents.
- **Documentar** tots **els incidents crítics i alts** conforme els processos i **informes establerts**.

  Actualitzar i mantenir **els processos de gestió d'incidents** per als **5 principals tipus d'incidents.**

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.

2.5 REQUISITS DEL SERVEI

2.5.1 Gestió d'incidents

2.5.1.1 Resposta a incidents diligent, garantint que no torni a succeir en els àmbits d'actuació de l'Agència de Ciberseguretat.

Es desenvoluparan des de la prestació com a mínim les accions que es detallen a continuació, sempre seguint models estàndards i metodologies reconegudes internacionalment com per exemple la NIST 800-61.

- 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 evidències generades i/o recavades durant la fase d'atac, que prové del servei de Control i Operació del Perímetre de Seguretat i de la possible informació generada per l'equip d'Anàlisi de ciberamenaces, com pot ser reportada per tercers o el mateix afectat.

Els incidents de seguretat han d'estar tipificats segons el catàleg de ciberamenaces i vectors de l'Agència de Ciberseguretat, s'ha de categoritzar, etiquetar i registrar totes les dades associades.

- 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 trobar la línia del vector o vectors d'atac de l'incident que han provocat l'afectació, determinar el què, qui, com i el per què (motiu).

- 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 donar una finestra de temps per tal que l'equip de resposta enfront d'incidents 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.
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 de Ciberseguretat.
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 (p. ex.: Enginyeria), 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. Aquesta sol·licitud s'han de contrastar entre l'equip de resposta contra incidents i 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 (p. ex.: Enginyeria) 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. Aquesta sol·licitud cal contrastar entre l'equip de resposta a incidents i 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 enfront d'incidents s'ha d'adequar als temps de resposta mínims definits. 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 de Ciberseguretat, 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 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 que estén, 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 contramesures adients per eradicar els incidents.

Aquestes contramesures han d'estar dirigides a protegir la infraestructura afectada per l'incident en qüestió 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 portar a terme aquestes contramesures s'ha de contar tant amb els equips de l'àmbit de Protecció com de Resposta contra incidents, interns o 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 seguretat del perímetre, i evitar que l'incident es torni a produir. Aquestes mesures s'han de comunicar a l'àmbit de protecció i a Anàlisi de Ciberamenaces per tal de millorar l'efectivitat del serveis.
S'ha de tenir un registre i fer un seguiment d'aquestes, 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.

2.5.1.2 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 cibercrimenals 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 en entorns complexos, on normalment les condicions per a realitzar una resposta a incidents no és idònia o entorns desconeguts. L'Agència de Ciberseguretat, 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 entorn nou.

2.5.1.3 Desenvolupament de la infraestructura per poder donar resposta.

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'evidencies.
    - 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.
- Análisis d'evidencies.
    - Tecnologies per a l'anàlisi d'evidències de data lake i SIEM en el núvol i físic.
- Contención de l'amença
    - 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 de Ciberseguretat i en el núvol.

El Servei licitat tindrà de **mantenir i evoluciar aquest ecosistema**. A més de **desenvolupar el cos procedimental i de govern** en els **7 àmbits d'actuació** de l'Agència perquè estiguin **degudament preparats en la resposta d'incidents**.

2.5.1.4 Resposta prioritzada segons els requisits d'intel·ligència i nivell de criticitat.

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 (Lot 2). 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.

2.5.1.5 Anàlisi forense de dispositius en entorns on premise, núvol i mòbils.

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

- És en aquest requisit a on es necessària tota la capacitat tècnica d'anàlisi forense en les diferents disciplines:
    - Network Forensics .
    - System Forensics (Windows / Linux&Unix / MacOSx / ...).
    - Mobile Forensics.
    - IOC extraction.

- 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 de Ciberseguretat. Mai cal fer aquesta anàlisi amb les dades originals, sempre s'utilitzaran còpies clonades d'aquestes dades.

És important que el prestador tingui un coneixement exhaustiu de l'inventari de les eines i solucions disponibles a l'Agència de Ciberseguretat, el seu estat d'actualització i llicenciament, com la capacitat necessària per fer-hi ús.

❖ 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 / Informe d'anàlisi forense). 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 que s'ha emmagatzemat en el registre de resultats cal tractar per a de definir una relació en comú entre les evidències analitzades i trobar una imatge comuna entre elles per tal de presentar uns resultats reveladors.
Addicionalment a la presentació dels resultats dels informes de forma estandarditzada utilitzant estàndards internacionals com els proposats pel *Mitre Security Standarts*, s'ha d'incloure un gràfic d'un model que reflecteixi la relació entre els diferents actors que intervenen en un incident de ciberseguretat, un dels possibles models que es pot utilitzar sèrie el conegut com a *Diamond Model*.

❖ Conclusions obtingudes.

Cal definir una plantilla preestablerta de presentació de les conclusions obtingudes mitjançant la presentació de resultats de l'anàlisi forense, la informació i les evidències adquirides.

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 pel Responsable del Servei (RLS), i realitzar-se subjecte a la normativa interna de l'Agència de Ciberseguretat.

2.5.1.6 *Anàlisi estàtic i dinàmic de mostres de malware.*

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 Ghrida i anàlisi dinàmic amb les diferents sandbox que disposa l'Agència de Ciberseguretat tant de codi obert com diversos fabricants.

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

2.5.1.7 *Manteniment i evolució de la documentació i processos de resposta.*

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 funcionalitat de poder compartir la informació de manera normalitzada amb tercers si és necessari.
Tota la informació registrada ha de seguir un estàndard de normalització com p.e *Mitre Security Standarts.*
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 5 principals tipus d'incidents gestionats habitualment han de tenir els seus respectius playbooks associats i actualitzats.

Els 7 àmbits d'actuació de l'Agència de Ciberseguretat i els seus proveïdors **han de tenir els procediments i metodologia de resposta** requerits per a estar preparats per a una resposta a incidents efectiva.

2.5.1.8 *Suport en el compliment normatiu i les polítiques de resposta a incidents.*

El Servei ajudarà amb el seu coneixement i experiència a millorar el marc normatiu de la Generalitat de Catalunya. Així com recomanar les millors polítiques de resposta a incidents en els set àmbits de l'Agència de Ciberseguretat, complementat amb la resta de requeriments, l'objectiu és establir diferents entorns preparats per a la resposta a incidents efectiva.

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)

2.5.2 Cerca proactiva d'incidents

2.5.2.1 Capacitat per a desenvolupar i executar freqüentment missions de cerca proactiva d'incidents

- Creació planificació i execució prioritzada del pla tecnològic per la recerca proactiva d'incidents.

  Es desenvoluparà un calendari anual amb les diferents missions objectiu, prioritzades i orientades a obtenir el millor resultat basant-se en les tècniques amb un major impacte.

- 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 de hunting 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.
- El resultat d'aquesta recerca ha d'aportar com a mínim:
  - La generació de nous casos d'ús, que es poden traduir en noves regles de correlació, IOC's, etc.
  - L'ús de determinades eines o scripts, etc.
  - La generació i adaptació de signatures de protecció del perímetre (Antivirus, IPS, Filtrat de Continguts, etc.).
  - La generació de noves regles en el SIEM o la modificació de les ja existents, incloent-hi l'ajust de llindars.
  - Generació d'indicadors de compromís, considerant p. ex. adreces IP, dominis, adreces de correu electrònic, noms d'usuari i noms de fitxers sospitosos.
  - La sol·licitud de registres d'esdeveniments més detallats i la seva integració en les eines de detecció per analitzar determinats tipus d'esdeveniments clau.
  - La proposta d'implantació de noves eines.
- Creació i revisió de casos d'ús per a alimentació del SOC.

  Es donarà suport a les altres línies de servei del Centre d'operacions 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.

- 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 a l'entorn de la Generalitat.

- Contextualització i comprensió d'escenaris.

  S'analitzaran els diferents escenaris tant interns com externs, així com identificar-los a la Generalitat de Catalunya i 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 fucnió d'Intel·ligència Operativa.

  Es realitzaran anàlisi d'amenaces desconegudes a la Generalitat de Catalunya 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 recerca proactiva d'incidents (threat hunting).

2.5.3 Gestió d'evidencies

2.5.3.1 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.

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

2.6 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 de Ciberseguretat. 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 capes més executives.

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

- Coordinació amb la resta d'àrees i equips de l'Agència de Ciberseguretat.
- Generació, implementació i càlcul de les mètriques i els indicadors del servei.
- Gestió de la capacitat del servei i la seva disponibilitat.
- 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 de Ciberseguretat 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, AOC, hospitals i 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 de Ciberseguretat de Catalunya les informacions objectives i subjectives que permetin a la Direcció la presa de decisions operatives, tàctiques i estratègiques relacionades amb el contracte.
- Quality assurance pel servei.
- Gestió de riscos operatius del servei.

El licitador designarà un **Cap de Servei**, descrit en aquest document, que serà el principal responsable del servei. Aquest responsable, en base al model de relació de l'Agència de Ciberseguretat, es coordinarà amb el Responsable de la Línia de Servei (RLS) de l'Agència de Ciberseguretat de la funció d'Intel·ligència Operativa, per tal de garantir la correcta execució de les capes de gestió, administració i servei.

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

2.7 ROLS I FUNCIONS

El licitador haurà de presentar el seu plantejament d'equips humans i la seva organització per tal de donar resposta a les necessitats i les funcions que l'Agència de Ciberseguretat demana amb el detall de dedicacions i perfils corresponents.

Tot i així, es descriuen al punt *4.4.2 de Perfils* alguns dels rols necessaris i les funcions assignades per tal de conformar l'equip que proporcioni els serveis de Resposta a Incidents, així com el perfil considerat més aconsellable per a desenvolupar-ho.

2.8 VOLUMETRIES ACTUALS

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

Concepte	Quantitat/any
Incidents molt complexos o APTs	**2**
Incidents per explotació vulnerabilitats 0 day	**2**
Incidents per cibercrim	**12**
Altres incidents no dirigits rellevants	**60**
Generals	
Aplicacions	**2.500**
Adreces IP en Sistemes d'Informació	**10.000**
Llocs de treball	**200.000**
Tràfic gestionat a la xarxa	**20 Gbps**
Seus Singulars	**3.622**
Escoles	**3.786**
Ajuntaments	**947**
Diputacions	**4**
Consells comarcals	**42**
Universitats públiques	**12**
Instituts universitaris d'investigació	**50**
Facultats i escoles universitàries	**187**
Centres d'investigació	**39**
Hospitals	**68**
Hospitals de referència	**8**
Consorcis	**16**
Gerències territorials	**9**
Organismes públics	**209**
Llocs web .CAT	**107.000**
Adreces IP dins de Catalunya	**350.000**

2.9 LLIURABLES DEL SERVEI

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

Entre els lliurables es poden considerar productes que inclouen la investigació d'incidents i el seu suport com a anàlisi forense o de malware, la seva presentació executiva, recerca proactiva d'incidents, resums de l'activitat dels serveis mensualment, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres.

En aquest sentit i derivat de l'importància de l'Agència de Ciberseguretat que atorga a la qualitat dels diferents lliurables del servei, el licitador haurà de presentar 2 exemples reals de cadascun dels tipus de lliurables presentats a continuació. Aquests documents hauran de presentar-se anonimitzats.

- Lliurable 1: Informe i quadre d'estat de servei
- Lliurable 2: Proposta de mètriques i indicadors de servei
- Lliurable 3: Informe d'incident, cas de compromís d'un actiu de tipus servidor, a on ha estat necessari realitzar més d'un tipus d'anàlisi forense.
- Lliurable 4: Informe tècnic d'un anàlisi forense de variant de codi maliciós.
- Lliurable 5: Informe d'anàlisi forense d'un dispositiu mòbil compromès.

2.9.1 Productes

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	Volumetria aprox./anual
Informe d'incident	Puntual	60
Presentació executiva d'incident	Puntual	20
Informe d'analisi forense	Puntual	25
Informe d'analisi de malware	Puntual	5
Fitxes de gestió d'incidents	Puntual	60
Fitxes execució de misiones de recerca proactiva d'incidents	Puntual	20
Informe de mètriques i indicadors de Servei per àmbit amb el resultat del seu anàlisi.	Puntual	12
Informe resum dels incidents gestionats en un àmbit concret, com pot ser un Departament de la Generalitat de Catalunya, Administració local, Ciutadania, etc. Anàlisi d'estat de situació amb propostes de millora en curs, i problemàtiques associades.	Periòdic	12
Informe d'anàlisi/problemàtica d'una tipologia determinada d'incident de seguretat, per exemple infeccions recurrents en un	Puntual	5

departament, compromís reiteratiu d'una tipologia d'actiu, etc.		

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 de Ciberseguretat. Els canvis s'acordaran entre l'adjudicatari i la pròpia Agència de Ciberseguretat, garantint no generar un impacte greu en cap de les dues parts.

2.9.2 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 Operativa",* funció encarregada de la construcció d'indicadors del SOC, totes aquelles mètriques requerides. Aquestes mètriques s'han de realitzar mitjançant les eines que es disposen des de l'Agència de Ciberseguretat.

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar per part del licitador. L'Agència de Ciberseguretat es reserva el dret de modificar aquest llistat de mètriques de manera acordada amb l'adjudicatari.

Aspecte mesurat	Descripció
Activitat Gestionada	Nombre, tipologia i ambit de les peticions gestionades pel servei
Gestió d'incidents duts a terme	Gestió d'incidents realitzats en el mes en curs
Missions de recerca proactiva d'incidents	Nombre d'exercicis completats de recerca proactiva d'incidents
Inventari d'evidencies	Nombre, tipologia i data de les evidencies adquirides.

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

- Nombre de tiquets en el servei.
- Dates d'inici i de lliurament pactat i real de projectes.
- Puntuacions de satisfacció de lliurables.

2.10 MILLORA DELS SERVEIS

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

Alguns exemples a tenir en compte són:

- Millora de la metodologia de treball del servei.
- Millora dels productes a lliurar.
- Reducció dels temps de les tasques a realitzar.

- Optimització de les eines de treball.
- Millora de mètriques i indicadors operatius.
- Industrialització i automatització de processos.
- Millora d'eficiència i eficiència de processos, tecnologies, etc.

Totes les tasques de transformació seran sempre acordades, planificades i validades amb la funció *d'Evolució i Transformació* de l'Agència de Ciberseguretat.

3 LOT 2: SERVEI DE SUPORT D'INTEL·LIGÈNCIA OPERATIVA

L'objectiu principal de la funció d'Intel·ligència Operativa es el de proveir el coneixement i els plans de actuació necessaris per permetre reduir, de manera efectiva i eficient, l'afectació de les ciberamenaces dins dels àmbits d'actuació. Per tal de fer front a aquesta encomana, des del servei de suport licitat al Lot 2 s'ha de realitzar la feina de processar la informació provinent tant de la resta de funcions (*Control i Operació del Perímetre*, *Resposta Activa*, etc.), com informació de context disponible tant de les fonts internes com les externes, per tal de convertir-la en un producte que habiliti la presa de decisions.

Les tasques a realitzar han de permetre generar criteri sobre ciberamenaces que puguin esdevenir un potencial incident de seguretat en cas de ser dirigides als clients als que l'Agència de Ciberseguretat presta servei. Els resultats es produeixen a partir de la recerca i correlació de la informació existent en totes aquelles fonts accessibles per l'Agència de Ciberseguretat i serveixen de base per fer un seguiment i disposar d'un històric de les ciberamenaces identificades.

La detecció d'aquestes ciberamenaces permet a l'Agència de Ciberseguretat:

- Assegurar un alt **grau de cobertura de totes les amenaces actives rellevants**, orientant la execució d'un seguit de tasques que garanteixen una prevenció d'amenaces òptima i una resposta més eficient en front a incidents.
- Generar **relat adequat per les capes executives**, que es pot alinear de manera natural amb conceptes com el risc, les inversions o altres problemes coneguts.
- **Influir en la priorització** de la mitigació de les vulnerabilitats, aportant per exemple una motivació clara per justificar l'aplicació urgent de certs pegats.
- Reduir la **"fatiga d'alerta"** i afegir context als indicadors tècnics disponibles.
- Definir el **camí de la evolució i la millora** dins del SOC/CERT, segons el conjunt de ciberamenaces gestionades i la efectivitat i la eficiència mesurades al prevenir-les i respondre davant els incidents associats.
- Adequar de manera anticipada les estratègies de resposta disponibles, dins d'un concepte ***"de Threat&Incident Readiness"***, per avançar la preparació davant d'un incident o d'una amenaça.

- **Determinar el nivell d'exposició** dels diferents clients de l'Agència de Ciberseguretat en vers una ciberamenaça detectada.
- Anticipar-se adequadament en la **revisió de l'efectivitat dels controls** actuals de seguretat desplegats.
- **Orientar l'orquestració operativa de tot el SOC/CERT** per garantir que els recursos disponibles es concentren als focus operatius adequats en tot moment.
- Desenvolupar un **Programa d'Intel·ligència de Ciberamenaces** per poder compartir amb altres actors externs coneixement, Intel·ligència accionable i tecnologia específica.
- **Informar** als possibles organismes, entitats afectades i proveïdors de servei per tal que puguin prevenir i respondre de manera efectiva i eficient.

Cal destacar que l'Agència de Ciberseguretat actualment disposa d'un laboratori de seguretat en el que es poden explotar eines amb l'objectiu de facilitar les tasques relatives al servei en qüestió, de les següents tipologies:

- Adquisició d'evidències i anàlisi forense.
- Anàlisi d'artefactes i codi maliciós.
- Estudi de contramesures i anàlisi de tràfic.
- Investigació d'actors i tècniques OSINT.

3.1 OBJECTE DE LA LICITACIÓ

El servei licitat inclou les tasques de suport a la funció d'Intel·ligència Operativa i les seves subfuncions, que han de permetre l'assoliment de tots els objectius definits per l'Agència de Ciberseguretat de Catalunya.

3.2 ORIENTACIÓ

, El licitador haurà de contemplar els següents principis que son els que regeixen el disseny del present servei de suport i la seva licitació:

- El servei **es valorarà principalment pels seus resultats, que han de ser excel·lents**. Al present document s'evita explícitament requerir la inclusió per part del licitador de informació sobre els perfils específics o la quantitat d'hores que es requeriran per assolir cadascun dels objectius definits. L'adjudicatari no està obligat a compartir aquest detalls i conseqüentment serà el principal responsable de la qualitat final del servei i de la consecució de les fites marcades, quedant l'Agència de Ciberseguretat com a **consumidor** dels resultats a nivell operatiu.
- En aquesta línia, el servei ha de ser completament autosuficient, **minimitzant l'adjudicatari les dependències** amb el personal de l'Agència de Ciberseguretat per executar les tasques al seu dia a dia.
- De la mateixa manera, el servei ha d'estar **totalment alineat amb les necessitats de la funció d'Intel·ligència Operativa**, adaptant-se al context de l'Agència de Ciberseguretat, al seu entorn i al de els seus àmbits d'actuació.

- El servei de suport d'Intel·ligència Operativa forma part d'un equip més global com és el SOC/CERT i com a tal s'ha d'assegurar en tot moment la **complerta integració operativa** amb la resta de serveis de suport i de funcions.
- Els resultats generats pel servei han d'habilitar, de manera natural, la **presa de decisions**, tant a nivell operatiu, com tàctic i estratègic.
- El servei ha de donar suport a l'Agència de Ciberseguretat de Catalunya en el **posicionament internacional** del Catalonia CERT, com a referent de ciberseguretat.

3.3 DESCRIPCIÓ

El servei de suport d'Intel·ligència Operativa realitza tasques proactives respecte al resultat de l'operació dels serveis de prevenció, de protecció i resposta, incloent-hi informació de context i d'altres fonts d'informació per tal d'identificar correlacions entre ciberamenaces que puguin esdevenir o esdevinguin un incident de seguretat per als actius sota l'abast de l'operació de la seguretat de l'Agència de Ciberseguretat.

Les subfuncions d'Intel·ligència Operativa són les següents:

- Pronòstic i Investigació de Ciberamenaces
- Estratègia de Resposta
- Orquestració i context

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

3.4 OBJECTIUS DEL SERVEI

El present apartat inclou un llistat d'objectius 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.

- Identificació del Catalonia CERT com a principal **referent de ciberseguretat** dins del territori i fins al TOP 3 a Espanya i el TOP 10 a nivell europeu.
- **Establiment de canals dedicats per cadascun dels àmbits d'actuació definits** per proveir coneixement que els permeti prevenir amenaces i respondre en front a incidents de manera efectiva i eficient. Aquest coneixement ha de ser el **resultat de l'anàlisi del 100% de l'activitat operativa** rellevant del SOC/CERT. En aquest cas a més, els graus d'eficàcia, d'eficiència o de satisfacció per reduir l'afectació de les ciberamenaces ha de ser superior al 80%.
- **Definició dels models d'avaluació d'exposició a l'amenaça** pels **5 principals tipus d'actiu de cadascun dels àmbits d'actuació,** que permetin informar als clients de l'Agència de Ciberseguretat de quines son les principals amenaces que podrien afectar-los. Un mateix model no té perquè ser exclusiu per un únic àmbit i es pot reaprofitar en més d'un.
- **Desenvolupament i gestió de les estratègies de resposta** adients pels **5 principals tipus d'incident i pels 5 principals tipus de ciberamenaça** per cadascun del **àmbits d'actuació**. Les estratègies han d'haver estat activament

validades amb garanties. Una estratègia de resposta no té perquè ser exclusiva per un únic àmbit i es pot reaprofitar en més d'un.

- Establiment d'almenys **8 acords de col·laboració per any** amb altres actors externs dins del context del **Programa d'Intercanvi d'Intel·ligència de Ciberamenaces** de l'Agència de Ciberseguretat de Catalunya.
- **Detecció proactiva d'esdeveniments rellevants** per tots **7 àmbits** d'actuació amb un rati d'efectivitat **no inferior al 90% en un període d'un mes.**
- **Infraestructura** requerida per habilitar dins del SOC/CERT un **ecosistema d'intercanvi d'intel·ligència de ciberamenaces** amb actors externs adscrits al Programa d'Intercanvi d'Intel·ligència de Ciberamenaces de l'Agència de Ciberseguretat de Catalunya. Aquesta infraestructura, juntament amb els procesos adients, ha de estar completament desplegada i operada per part del servei de suport.
- La ciberamenaça ha de ser el **element vehicular** per almenys el **90% de tota l'activitat operativa** executada dins del SOC/CERT, reforçant el concepte d'una operació "Threat Centric".

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 valorarà molt positivament la viabilitat del pla proposat, la reducció dels temps requerits per assolir els objectius i la millora qualitativa d'aquests mateixos objectius.

3.5 REQUISITS DEL SERVEI

3.5.1 Pronòstic i investigació de ciberamenaces

3.5.1.1 Pronòstic de ciberamenaces actualitzat i especialitzat per àmbit en temps real.

L'anàlisi de tota la informació que es recull i genera, tant internament com per a tercers, ha de tenir com a objectiu la correlació, ordenació, normalització i interpretació de les dades i evidencies, per tal d'aconseguir una imatge general de la seguretat enfront de les ciberamenaces adaptada a cada client, personalitzant el missatge i transmetent un relat fonamentalment rellevant pel receptor.

Per cadascun dels àmbits d'actuació definits, el servei licitat ha de ser capaç de descriure, en qualsevol moment, l'estat de les ciberamenaces actualment més rellevants, atenent, entre d'altres, el seu grau de bel·ligerància contra l'àmbit, la seva capacitat tècnica, la naturalesa dels objectius perseguits o el grau de focalització específic contra l'àmbit en qüestió.

El conjunt d'amenaces identificades com a rellevants composa el que l'Agència de Ciberseguretat denomina el *"Threat landscape"* d'un àmbit (segons el termini en anglès) i permet filtrar l'excés d'informació disponible sobre ciberseguretat i la seva actualitat i identificar només les ciberamenaces que poden afectar a l'àmbit amb una major probabilitat i que per tant han de ser ateses de manera prioritària.

En definitiva, el que s'ofereix és un anàlisi del comportament de les ciberamenaces actualment actives, fent focus en aquelles més rellevants, perquè es preveu poden afectar a l'àmbit, incloent detalls sobre la seva naturalesa i aportant les eines necessàries per poder prevenir-les, tant a nivell tècnic, com operacional, tàctic i, fins i tot, estratègic.

A més, s'aporta una previsió del comportament d'aquestes amenaces, per poder justificar la presa de decisions i possibilitar la adequació dels plans de resposta de manera anticipada.

3.5.1.2 Càlcul del grau d'exposició a l'amenaça dels actius de l'àmbit.

A partir del coneixement disponible sobre les ciberamenaces més rellevants que afecten a l'àmbit al que pertany un determinat actiu o un conglomerat d'actius, el servei licitat ha de poder ralitzar un anàlisi i valorar quina afectació potencial podrien generar amb més probabilitat les ciberamenaces identificades.

Aquesta anàlisi es construeix sobre proves tècniques de diversa profunditat prèviament disponibles des d'altres fonts que queden fora de l'abast de la present licitació (escaneigs de vulnerabilitats web, simulacres de phishing, anàlisis Wifi, etc.) i es focalitza en estudiar la superfície d'exposició existent i la pròpia naturalesa dels elements implicats (com per exemple, quins processos de negoci es troben involucrats) per, en definitiva, identificar entre d'altres: quin tipus d'adversari podria tenir interès en realitzar un atac, amb quina finalitat ho faria o també amb quins vectors d'atac i eines.

A partir del coneixement disponible, d'una banda, sobre el conjunt d'elements analitzats i, d'altra, sobre el conjunt de ciberamenaces rellevants, el servei ha de calcular l'estat d'alerta pels actius sota anàlisi.

El resultat d'aquest exercici permet, entre d'altres, prioritzar les tasques de prevenció adients per cada ciberamenaça i identificar les contramesures òptimes en cada cas, proveint un argument sòlid per motivar la execució de les tasques associades.

El grau d'exposició a l'amenaça es pot calcular contra un ampli ventall de tipus d'entitats: Des d'un sistema d'informació aïllat, un grup d'usuaris com per exemple tot el personal d'un organisme públic o fins i tot contra tots els elements que participen d'un operatiu electoral. En casos com aquest últim, sovint es requereix una avaluació recurrent de la exposició a l'amenaça durant un període de temps limitat, per poder avaluar la evolució de la exposició de manera continua.

En aquest punt, resulta obvi que la naturalesa dels elements a analitzar pot arribar a ser realment diversa i per tant, el servei licitat ha de disposar de diferents models per transmetre eficaçment els resultats de l'anàlisi per tots els àmbits d'actuació, al menys pels principals tipus d'actius de cadascun.

El servei de suport licitat haurà de definir, mantenir i evolucionar aquests models, que permetran a l'Agència de Ciberseguretat de Catalunya avaluar, de manera puntual o recurrent, el grau d'exposició a l'amenaça per la major part de tots els seus àmbits d'actuació.

3.5.1.3 Requisits d'Intel·ligència Prioritzats recurrents i sota demanda

Actualment l'Agència de Ciberseguretat de Catalunya disposa del seu propi repositori de requisits d'Intel·ligència de Ciberamenaces on s'organitzen les principals necessitats de coneixement identificades. Aquestes necessitats queden definides de manera que el repositori inclou detalls sobre quines son "les principals preguntes a contestar" per part de la funció, dins de quins productes d'Intel·ligència o a partir de quina informació recollida des de fonts internes o externes.

El repositori conté tant requisits recurrents com els ad-hoc més freqüents i inclou requisits per totes les dimensions contemplades al SOC/CERT, com ara: Intel·ligència Tècnica, Tàctica, Operacional i Estratègica.

Per tal de poder satisfer molts d'aquests requisits, el servei licitat ha de disposar d'Intel·ligència d'Amenaces rellevant, detallada i accionable, obtinguda des de fonts de qualitat amb continguts generats a partir d'amenaces i incidents rellevants al món i en particular al territori de Catalunya. El servei haurà de garantir l'accés a aquesta Intel·ligència a la resta d'analistes i membres del SOC/CERT.

De manera puntual i relacionat amb els requisits que poden plantejar-se **sota demanda**, davant d'una situació de crisi rellevant (bé sigui un incident de seguretat o una ciberamenaça), el servei haurà d'estar capacitat per participar en un "*squad*" dedicat i donar suport, proveint context i satisfent les necessitats de coneixement que es generin.

L'adjudicatari serà el principal responsable del repositori de requisits disponible a Intel·ligència Operativa i com a tal, haurà de mantenir-ho, executant tasques de revisió al menys dues vegades al any i satisfer els requisits definits dins dels límits temporals fixats per cada requisit. Durant el procés de revisió, els canvis proposats s'hauran d'acordar amb el *Responsable de la Línia de Servei (RLS)* de l'Agència de Ciberseguretat de la funció d'Intel·ligència Operativa.

En cada moment, el conjunt de productes a generar haurà de ser acordat entre el servei de suport i els responsables interns de l'Agència de Ciberseguretat.

3.5.1.1 Detecció d'esdeveniments rellevants per a la prevenció i la resposta en front a amenaces

El servei licitat haurà de detectar determinats esdeveniments, que puguin resultar **rellevants** des del punt de vista de la prevenció i la resposta en front a amenaces dins **de tots els àmbits d'actuació** de l'Agència de Ciberseguretat de Catalunya, com a mínim:

- La venda de **credencials vàlides en fòrums cibercriminals** que permetin l'accés il·legítim a una infraestructura corporativa.
- El compromís i la subsegüent **alteració no autoritzada d'un lloc web**.
- La publicació d'infraestructura maliciosa amb la finalitat de llançar un **atac de suplantació** contra un lloc web legítim.
- La **publicació en xarxes socials** de continguts que denotin la materialització d'un incident.
- **La publicació en fonts públiques** de dades potencialment sensibles, com fitxers interns de configuració pertanyents a sistemes d'informació.
- **La publicació de leaks** d'informació amb credencials o informació sensible rellevant.
- La inclusió d'infraestructura legítima en una **blacklist.**
- La publicació d'una **aplicació mòbil maliciosa** que suplanti una aplicació legítima.
- De manera general, **la preparació d'un atac** contra actius d'un dels àmbits d'actuació.

El licitador podrà proposar un conjunt de tipus d'esdeveniments rellevants a detectar diferent per cada àmbit d'actuació.

En aquesta línia, el servei licitat ha de ser capaç de detectar esdeveniments rellevants i generar la corresponent alerta a processar dins del SOC/CERT, però idealment també ha de disposar de la capacitat per executar **cerques sota demanda** d'elements específics a totes les fonts disponibles.

3.5.1.2 Suport en la interacció del Catalonia CERT amb tercers

El Catalonia CERT articula la creació d'una xarxa de compartició d'informació arreu del seu **Programa d'Intercanvi d'Intel·ligència d'Amenaces** propi, habilitant rebre Intel·ligència d'Amenaces rellevant pels àmbits, però més prioritàriament, permetin proveir als participants del Programa amb continguts de valor que contribueixin a millorar les seves capacitats per prevenir amenaces i respondre enfront d'incidents de ciberseguretat.

El servei licitat ha de donar suport al personal intern de l'Agència de Ciberseguretat en les tasques **de promoció i desenvolupament del Programa d'Intercanvi d'Intel·ligència d'Amenaces** propi de l'Agència de Ciberseguretat de Catalunya i ha de col·laborar en la definició i la execució d'una **estratègia** per establir i explotar nous canals de cooperació amb altres SOCs, CERTs, fabricants, Centres especials de seguretat, laboratoris i experts investigadors del mon de la ciberseguretat.

En la mateixa línia, el servei de suport serà el principal responsable de la **comunicació del Catalonia CERT amb elements externs** com poden ser altres CSIRTs/CERTs, col·laboradors o fins i tot tercers que per exemple reportin vulnerabilitats als àmbits. Això no va en detriment de que altres funcions del SOC/CERT puguin contactar en nom del Catalonia CERT amb actors externs, com per exemple l'equip de Resposta Activa, durant la gestió d'un incident que requereixi la coordinació amb altres equips de resposta aliens a l'Agència de Ciberseguretat o el propi equip de Control i Operació, per coordinar l'aplicació de les mesures de mitigació necessàries per prevenir una ciberamenaça específica.

3.5.1.3 Desenvolupament de la infraestructura per un ecosistema d'intercanvi

El SOC/CERT ha de disposar d'una infraestructura que habiliti l'intercanvi d'intel·ligència de ciberamenaces amb altres actors externs, particularment amb tercers adscrits al Programa de d'Intercanvi d'Intel·ligència de Ciberamenaces de l'Agència de Ciberseguretat.

Actualment, dins del SOC/CERT, ja existeix un ecosistema de la mateixa naturalesa, composat per diferents solucions tecnològiques i processos, que proveeixen les següents capacitats:

- Compartició d'Intel·ligència de Ciberamenaces de diferents nivells amb tercers externs adscrits al Programa CTI de l'Agència de Ciberseguretat.
- Gestió d'una base d'usuaris adscrits al Programa CTI de l'Agència de Ciberseguretat.
- Anàlisi tècnic d'amenaces: anàlisi de la infraestructura atacant, eines i vulnerabilitats aprofitades, victimologia, etc.
- Consolidació i neteja de tota la Intel·ligència Tècnica rebuda des de totes les fonts accessibles per l'Agència de Ciberseguretat, que pugui ser consumida entre d'altres pel propi SOC/CERT.
- Cerca retrospectiva i automatizada d'activitat maliciosa a l'àmbit a partir d'indicadors reportats per d'altres des de fonts externes.

El següent és un llistat de tecnologies rellevants que composen l'ecosistema d'intercanvi actual:

- MISP.
- Elastic Stack.
- SFTP.
- Agregador d'Intel·ligència d'Amenaces (desenvolupament intern).
- SOAR.

L'adjudicatari ha d'assegurar que l'Agència de Ciberseguretat i específicament el SOC/CERT, mantenen i també evolucionen les capacitats actuals referides anteriorment.

Cal tenir en compte els principals canals per distribuir coneixement cap als àmbits d'actuació, el detall de quina infraestructura i processos suportaran aquesta acció i la estratègia per desenvolupar els mitjans i les capacitats requerides.

El model proposat pel licitador per transmetre efectivament un pronòstic de ciberamenaces personalitzat a cada àmbit, incloent la previsió del seu comportament i el coneixement necessari per permetre reduir, de manera efectiva i eficient, l'afectació de les ciberamenaces. La proposta del licitador per poder liderar i coordinar la recollida de tota la informació necessària des de les fonts oportunes, com per exemple: altres funcions del SOC/CERT, proveïdors de CTTI o els propis clients segons els diferents àmbits. El model de producte a generar per lliurar el missatge desitjat, detallant els principals continguts a incloure o la justificació del model definit. El licitador haurà d'aportar un exemple de producte o alternativament una proposta d'estructura d'un model d'exemple, per complementar la seva proposta.

Es tindrà en consideració, proposta de Requisits d'Intel·ligència, que a criteri del licitador i a partir de la seva experiència i coneixement, haurien de definir-se per tota la funció amb l'objectiu de maximitzar el valor generat des del servei. El model operatiu, incloent processos, canals de comunicació, etc. per assegurar que la Intel·ligència de Ciberamenaces (tant tècnica, com operativa, com tàctica o estratègica) flueix de manera continuada fins a la resta d'equips del SOC/CERT, en temps i forma, garantint que aquesta Intel·ligència els permet reduir l'afectació de les ciberamenaces. La proposta dels esdeveniments rellevants a detectar per cada àmbit, atenent la justificació del tipus d'esdeveniment i del tipus de font o les fonts específiques a monitoritzar. Es valorarà més positivament una proposta que cobreixi més tipus d'esdeveniments que es considerin de valor, amb un major grau de qualitat de la detecció en termes de detall d'informació i de temps de reacció. Particularment rellevant serà la proposta de com s'integraran aquestes capacitats de detecció dins del model operatiu de tot el SOC/CERT. I la capacitat per, a més de generar alertes de manera proactiva arrel d'esdeveniments rellevants, satisfer sota demanda requeriments d'informació específics contra las fonts monitoritzades, generats per altres funcions i serveis del SOC/CERT durant la execució dels seus anàlisis i investigacions.

Cal exposar elements per donar suport en el desenvolupament del Programa d'Intercanvi d'Intel·ligència d'Amenaces de l'Agència de Ciberseguretat de Catalunya i per establir i aprofitar nous canals de comunicació amb altres entitats col·laboradores. La proposta per part del licitador per garantir l'aprofitament intensiu dels acords disponibles dins de l'Agència de Ciberseguretat i de les oportunitats de col·laboració que representen. I la gestió de les comunicacions cap al exterior des del CERT, identificant un model de coordinació entre els diferents serveis i funcions.

Es tindrà en consideració els aspectesi elements proposats per assumir la responsabilitat per part de l'adjudicatari sobre la infraestructura que dona suport al ecosistema CTI dins de l'Agència de Ciberseguretat, assegurant la seva integració al funcionament recurrent del servei. També les millores proposades a l'actual ecosistema.

3.5.2 Estratègia de resposta

3.5.2.1 Disseny i implementació de les estratègies de resposta adients per afrontar les ciberamenaces

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

Els plans han d'adreçar **les principals situacions de crisi** que es puguin esdevenir per cadascun dels àmbits d'actuació definits, bé siguin originades per un incident de ciberseguretat amb afectació ja confirmada o per una ciberamenaça que potser encara no s'ha materialitzat.

S'espera que els plans de resposta contenguin diferents nivells de detall referents a les tasques a executar en una situació de crisi, des de la part més operativa per definir com portar a terme tasques tècniques, fins a accions de més alt nivell que afectin al model de relació del SOC/CERT amb altres actors externs com els seus clients o altres entitats rellevants, com per exemple les autoritats competents.

En funció de la naturalesa d'una estratègia de resposta, el servei licitat podrà coordinar-se per trobar **recolzament a altres funcions i serveis de suport,** dins del SOC/CERT, que disposin d'un coneixement expert. Així per exemple, el desenvolupament d'un pla d'actuació enfront a un determinat incident es pot definir conjuntament amb l'equip de *Resposta Activa*, que segurament disposarà d'un coneixement més detallat i específic a nivell operatiu, tot i que el responsable últim d'aquesta estratègia serà sempre *Intel·ligència Operativa*.

3.5.2.2 Validació activa de les estratègies de resposta

El servei licitat haurà d'implementar els mecanismes necessaris per **validar de manera activa** les estratègies de resposta disponibles per cadascun dels àmbits, per tal d'assegurar de manera anticipada que estan correctament definides.

Es tindran en consideració les capacitats ja existents del licitador per desenvolupar estratègies de resposta. En aquesta línia, també es tindrà en consideració l'estructura i els continguts proposats pel licitador pels diferents tipus d'estratègies de resposta identificats, així com els processos establerts per assegurar el seu manteniment i evolució. El licitador haurà d'aportar la estructura d'una estratègia estàndard, a tall d'exemple, per complementar la seva proposta. I si el licitador ja disposa d'una col·lecció de plans d'actuació com els requerits que pugui introduir al servei. El licitador haurà d'aportar un exemple complert d'estratègia ja disponible, adientment anonimitzada, per complementar la seva proposta. El licitador haurà d'especificar quins mecanismes proposa per validar les diferents estratègies de resposta disponibles, contemplant diferents situacions i circumstàncies.

3.5.3 Orquestració i context

3.5.3.1 Orquestració operativa

Donat que la funció d'Intel·ligència Operativa es considera la primera experta en ciberamenaces dins del SOC/CERT, també s'identifica com la principal garant del model *"Threat Centric"* implementat entre totes les funcions. El servei licitat, per tant, ha de vetllar (i de proposar els mecanismes per que així sigui) per una coordinació efectiva entre tots els equips i per un enfoc operatiu amb l'amenaça com a element vehicular.

D'igual manera, el servei de suport ha de garantir que les estratègies de resposta disponibles s'executen segons la seva definició durant la gestió de crisis i durant la orquestració periòdica. Referent a aquest últim punt, dins del SOC/CERT tots els equips es reuneixen dues vegades cada dia per fer seguiment dels focus operatius, evolutius i incidentals. El servei de suport d'Intel·ligència Operativa, tot i no ser el encarregat de dirigir les reunions d'orquestració, sí que ha de complir un paper essencial, assegurant que les tasques realitzades pel SOC/CERT son òptimes per prevenir l'amenaça i respondre diligentment.

3.5.3.2 *Integració del context operatiu*

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

A tall d'exemple, la publicació d'una nova aplicació mòbil per part d'un Departament de la Generalitat de Catalunya i la corresponent campanya de comunicació orientada cap a ciutadania, pot ser rellevant pel SOC/CERT, especialment si aquest fet pot derivar en un increment del numero d'atacs rebuts per l'aplicació i el seu sistema d'informació associat. El servei de suport a Intel·ligència Operativa ha d'establir els mecanismes per que tots els elements que defineixen l'actualitat rellevant i que composen el context operatiu arreu dels àmbit d'actuació, puguin integrar-se al SOC/CERT i el seu dia a dia.

Cal tenir en compte els processos i els mecanismes necessaris, per participar en les reunions d'orquestració i articular la col·laboració amb tots els seus participants, contribuint a una operació orientada arreu del concepte de ciberamenaça. Haurà de detallar la seva proposta per integrar el context operatiu més rellevant dins del SOC/CERT de manera continua, generant la mínima sobrecarrega possible per la resta dels equips i desestimant aquells esdeveniments que puguin considerar-se soroll operatiu i per tant no rellevants per les funcions.

3.6 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 de Ciberseguretat. 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 capes més executives.

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

- Coordinació amb la resta d'àrees i equips de l'Agència de Ciberseguretat.
- Generació, implementació i càlcul de les mètriques i els indicadors del servei.
- Gestió de la capacitat del servei i la seva disponibilitat.
- 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 de Ciberseguretat 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, AOC, hospitals i 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 de Ciberseguretat de Catalunya les informacions objectives i subjectives que permetin a la Direcció la presa de decisions operatives, tàctiques i estratègiques relacionades amb el contracte.
- Quality assurance pel servei.
- Gestió de riscos operatius del servei.

Caldrà posar en valor tot el treball desenvolupat des del servei de suport i la funció d'Intel·ligència Operativa, particularment de cara a consumidors més executius com les Direccions corresponents dins de l'Agència de Ciberseguretat, el propi negoci o altres clients externs.

El licitador designarà un **Cap de Servei**, descrit en aquest document, que serà el principal responsable del servei. Aquest responsable, en base al model de relació de l'Agència de Ciberseguretat, es coordinarà amb el Responsable de la Línia de Servei (RLS) de l'Agència de Ciberseguretat de la funció d'Intel·ligència Operativa, per tal de garantir la correcta execució de les capes de gestió, administració i servei.

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

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

3.7 ROLS I FUNCIONS

Donat que el principal mecanisme d'avaluació de la qualitat del servei se centrarà en avaluar de manera continua els resultats generats pel servei i la seva adequació als acords establerts de manera conjunta entre l'Agència de Ciberseguretat i l'adjudicatari, no es requereix al licitador identificar un conjunt de perfils específics dedicats al servei, disposant de la flexibilitat per implicar els recursos necessaris per mantenir en tot moment el nivell de qualitat de servei exigit, de manera transparent a l'Agència de Ciberseguretat de Catalunya.

3.8 VOLUMETRIES ACTUALS

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

Concepte	Quantitat/any
Amenaces externes gestionades	**1.000**
Amenaces internes gestionades	**600**
Pronòstic d'amenaces	**50**
Exposició a l'amenaça	**40**
Requisits Prioritzats d'Intel·ligència	**10**
Nombre de butlletins de seguretat	**20**
Esdeveniments detectats amb potencial impacte imminent crític	**20**
Credencials compromeses identificades	**30.000**
Informes de hacktivisme	**12**
Informes de tècniques de DoS	**12**
Requeriments d'Informació des del SOC/CERT	**150**
Generals	
Aplicacions	**2.500**
Adreces IP en Sistemes d'Informació	**10.000**
Llocs de treball	**200.000**
Tràfic gestionat a la xarxa	**20 Gbps**
Seus Singulars	**3.622**
Escoles	**3.786**
Ajuntaments	**947**
Diputacions	**4**
Consells comarcals	**42**
Universitats públiques	**12**
Instituts universitaris d'investigació	**50**
Facultats i escoles universitàries	**187**
Centres d'investigació	**39**
Hospitals	**68**
Hospitals de referència	**8**
Consorcis	**16**
Gerències territorials	**9**
Organismes públics	**209**
Llocs web .CAT	**107.000**
Adreces IP dins de Catalunya	**350.000**

3.9 LLIURABLES DEL SERVEI

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

Entre els lliurables es poden considerar productes que inclouen coneixement per prevenir i respondre enfront amenaces, estratègies de resposta, exercicis d'avaluació de la exposició a l'amenaça, pronòstics d'amenaces, resums de l'activitat dels serveis mensualment, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres.

3.9.1 Productes

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
Pronòstic de ciberamenaces per àmbit	Setmanal
Avaluació de la exposició a l'amenaça	Puntual
Informe de ciberamenaça	Puntual
Alerta de ciberseguretat	Puntual
Fitxes seguiment: amenaces, actors, vulnerabilitats i malware	Puntual
Casos d'us per millorar les capacitats de detecció	Puntual
Informe de hacktivisme	Trimestral
Informe d'estat denegacions de servei	Trimestral

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

El licitador ha d'incloure una proposta de productes a lliurar pel servei, definint entre d'altres la seva motivació i periodicitat. Es valorarà la capacitat del licitador per adequar el missatge al receptor, especialment quan estigui orientat a negoci. Es valorarà la capacitat del licitador per produir continguts de qualitat, amb informació rellevant disponible de manera exclusiva pel licitador. El licitador haurà d'aportar algun producte anonimitzat, a tall d'exemple, per complementar la seva proposta.

L'adjudicatari participarà, juntament amb el personal de l'Agència de Ciberseguretat de Catalunya, i del SOC/CERT en particular, en la definició del catàleg de peticions de serveis de tot el SOC/CERT. Més específicament, Intel·ligència Operativa es el principal propietari del servei d'Exposició a l'Amenaça i com a tal es un dels principals responsables de definir aspectes del catàleg rellevants de cara als seus clients, com a: temps de resposta, cost, requeriments d'entrada, etc.

Caldrà tenir en compte la capacitat per generar productes alineats als diferents consumidors del servei d'Exposició a l'Amenaça, adaptant en cada cas les seves característiques, com podrien ser, a tall d'exemple: el contenidor del relat i el seu format, el tipus de llenguatge emprat o fins i tot l'idioma.

3.9.2 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 Operativa",* funció encarregada de la construcció d'indicadors del SOC, totes aquelles mètriques requerides. Aquestes mètriques s'han de realitzar mitjançant les eines que es disposen des de l'Agència de Ciberseguretat.

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar per part del licitador. L'Agència de Ciberseguretat es reserva el dret de modificar aquest llistat de mètriques de manera acordada amb l'adjudicatari.

Aspecte mesurat	Descripció
Activitat Gestionada	Nombre i tipologia de peticions gestionades pel servei
Investigacions dutes a terme	Investigacions realitzades en el mes en curs
Exposició a l'amenaça	Nombre d'exercicis completats d'anàlisi de la exposició a l'amenaça
Pronòstic d'amenaces	Nombre de pronòstics d'amenaces lliurats.
Alertes analitzades	Nombre d'alertes analitzades per part del servei
Esdeveniments rellevants detectats	Nombre i tipus d'esdeveniment identificats per cada àmbit d'actuació que han habilitat la presa de decisions.
Estratègies de resposta	Nombre d'estratègies de resposta definides i validades activament

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

- Nombre de tiquets en el servei.
- Dates d'inici i de lliurament pactat i real de projectes.
- Puntuacions de satisfacció de lliurables.

Es tindrà en consideració el conjunt de mètriques i indicadors del servei que, en funció del seu enteniment i experiència, permeten mesurar de la forma més adient el valor generat pel servei i habiliten la presa de decisions i la orientació tàctica i estratègica del servei de suport i de la funció principal que sustenta.

3.10 MILLORA DELS SERVEIS

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

Alguns exemples a tenir en compte són:

- Millora de la metodologia de treball del servei.
- Millora dels productes a lliurar.
- Reducció dels temps de les tasques a realitzar.
- Optimització de les eines de treball.

- Millora de mètriques i indicadors operatius.
- Industrialització i automatització de processos.
- Millora d'eficiència i eficiència de processos, tecnologies, etc.

Totes les tasques de transformació seran sempre acordades, planificades i validades amb la funció *d'Evolució i Transformació* de l'Agència de Ciberseguretat.

4 CONDICIONS D'EXECUCIÓ

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

4.1 HORARI DEL SERVEI

L'adjudicatari haurà de cobrir els horaris descrits a continuació:

BLOC DE SERVEI LOT 1	Horari
Suport de Resposta Activa	12x5 (amb guardies nit i festius)

BLOC DE SERVEI LOT 2	Horari
Suport d'Intel·ligència Operativa	24x7 tots els dies de l'any

Es requereix que la prestació dels serveis objecte de licitació sigui continua durant els 12 mesos de l'any, es a dir, la capacitat requerida ha de ser la mateixa.

4.2 UBICACIÓ FÍSICA

4.2.1 Bloc de servei Lot 1: Servei de suport de Resposta Activa

Els equips prestataris dels serveis poden operar remotament o a les pròpies instal·lacions de l'adjudicatari. Puntualment es podran ubicar a les oficines de l'Agència de Ciberseguretat, ubicades a l'Hospitalet de Llobregat, podent aprofitar les capacitats de laboratori, o en alguna ubicació designada per l'Agència de Ciberseguretat, sempre i quan aquest fet sigui requerit per la direcció de l'Agència de Ciberseguretat.

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 de Ciberseguretat que poden estar ubicades a qualsevol part del territori de Catalunya.

Al llarg del contracte es podria requerir un canvi en la ubicació dels professionals entre els centres operatius de la Agència de Ciberseguretat, 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 tal i com es detalla en els apartats anteriors d'aquest document.

4.2.2 Bloc de servei Lot 2: Servei de suport d'Intel·ligència Operativa

Els serveis es podràn prestar, si així ho requereix l'Agència, des de les seves pròpies dependències. Les instal·lacions, edificis i dependències utilitzats per a la prestació d'aquest servei hauran de complir en qualsevol moment amb tots els requisits de construcció, habitabilitat, seguretat i ergonomia estipulats per la normativa de règim local del municipi a on es trobi, de la Generalitat de Catalunya i de l'Estat en la seva expressió més exigent.

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

4.3 EQUIPS DE TREBALL

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 garantia les tasques definides i han de mostrar les habilitats necessàries per tal d'integrar-se en un equip d'alt rendiment, com es el del SOC/CERT. A efectes enunciatius, el següent es un llistat de les habilitats que s'espera de l'equip responsable de la prestació del servei:

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Alt grau de proactivitat i autosuficiència.
- Destresa comunicativa e interpersonal.
- Capacitat de treballar en equip i col·laborar amb la resta de serveis.
- 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.

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

Amb independència del model organitzatiu proposat, l'adjudicatari haurà de destinar, per a cada un dels lots, 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 de Ciberseguretat.

Els licitadors hauran d'incloure en la seva proposta l'organigrama i esquemes d'equips definits per tal de donar resposta a les necessitats expressades en aquest plec i per pemetre mantenir un model de relació fluid amb la resta d'equips i personal de l' Agència de Ciberseguretat de Catalunya, incloent, i de forma nominal, el/les persones designades com a Cap de Servei.

4.3.1 Bloc de servei Lot 1: Servei de suport de Resposta Activa

Per al servei licitat dins del Lot 1, l'Agència de Ciberseguretat tindrà dret a exigir justificadament a l'adjudicatari el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència de Ciberseguretat al cap de servei. L'adjudicatari haurà de presentar en un termini

màxim de 10 dies a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució.

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 de Ciberseguretat 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.).**

L'excessiva rotació del personal podrà ser penalitzada per l'Agència de Ciberseguretat, segons s'especifica al capítol 7. Així mateix, 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 de Ciberseguretat 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 de Ciberseguretat amb la deguda antelació un pla de substitució i disposició de recursos que doni resposta a les necessitats de l'Agència de Ciberseguretat 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 de Ciberseguretat) donar un nivell creixent de qualitat i volumetria de servei amb els mateixos recursos, **el nombre mínim d'hores efectives necessàries** per l'execució dels serveis demanats en aquest plec és la següent:

BLOC DE SERVEI LOT 1	DIMENSIONAMENT MÍNIM (HORES)
Suport de Resposta Activa	7040 h

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

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

Lot1 - Suport de Resposta Activa	DISTRIBUCIÓ ORIENTATIVA
Expert en Incidents	25%
Tecnic de Resposta	50%
Tecnic de recerca proactiva d'incidents	25%

4.3.2 Bloc de servei Lot 2: Servei de suport d'Intel·ligència Operativa

Donada l'orientació eminent cap a servei, no es requereix una definició explícita del número d'hores, més enllà de la proposta de l'organigrama i esquemes d'equips definits per tal de

donar resposta a les necessitats expressades en aquest plec, com ja s'ha fet present en aquest apartat.

4.4 PERFILS

4.4.1 Bloc de servei Lot 1: Servei de suport de Resposta Activa

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

Perfil	Requisits
Gestor / CAP del Servei	• Coneixements en definició i millora de processos. • Coneixements en eines de reporting i quadres de comandament. • Experiència mínima de 5 anys en gestió de projectes i equips. • Certificacions de fonaments en els marcs metodològics més comuns (ITIL, ISO 20.000, Prince2, COBIT, PMP o similar). • Certificacions de seguretat CISSM, CISSP, ISO 27.000, entre d'altres. • Nivell alt o mitjà d'anglès. • Titulat universitari en informàtica, telecomunicacions o similars en l'àmbit TI.
Expert d'incidents	• 5 anys o més d'experiència demostrable en el món de la seguretat. • Experiència demostrable en gestionar Equips tècnics de Resposta enfront d'Incidents. • 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. • Experiència en gestió de cadena de custòdia. • Coneixement de la legislació i normatives vigents en l'àmbit de la gestió d'incidents. • Certificacions valorables: GIAC, CISSP, OSCP, SANS SEC-401 o similars. • Capacitat proactiva, resolutiva i dots de lideratge.
Tècnic de resposta enfront d'incidents	• 5 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. • Certificacions valorables: GIAC, CISSP, OSCP, SANS SEC-401 o similars. • Capacitat proactiva i resolutiva.
Tècnic de 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. • Certificacions valorables: OSCP, CEH, GIAC o similars. • Capacitat proactiva i resolutiva.

4.4.2 Bloc de servei Lot 2: Servei de suport d'Intel·ligència Operativa

Donada l'orientació eminent cap a servei, no es defineix de manera explícita els perfils específics que l'adjudicatari implicarà per executar el servei.

4.5 IDIOMA DEL SERVEI

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

4.6 EINES

Els licitadors del contracte objecte d'aquest expedient hauran de presentar conjuntament amb la descripció del servei, i en els casos que sigui necessari, l'estratègia de les eines que li donaran suport.

Aquesta estratègia tindrà en compte:

- Manteniment i adequació de les eines actuals.
- Incorporació de noves eines, si fos adient.

Per tant, seguint aquesta estratègia, l'adjudicatari haurà de:

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

En el cas en què el licitador ho consideri necessari podrà plantejar la incorporació de noves eines per desenvolupar les seves funcions, explicant amb detall com les noves eines donen valor al servei i a l'Agència de Ciberseguretat de Catalunya tenint en compte els objectius de celeritat en la prestació dels serveis, així com la d'aprofitar sinergies i eficiències econòmiques. En aquest cas, es valorarà positivament que les eines proposades per a

incorporar a l'Agència de Ciberseguretat de Catalunya siguin "de mercat" en lloc de propietàries.

En aquest cas, el licitador detallarà, de manera separada, en la seva oferta econòmica el cost total i en tots els seus aspectes (adquisició, cessió, instal·lació, posada en marxa, formació, manteniment de llicències i suport, manteniment de llicències un cop finalitzada la fase de devolució del servei, etc.) de les eines que aporta, tenint en compte que aquestes eines i llicències seran per l'ús exclusiu de l'Agència de Ciberseguretat de Catalunya i que hauran de ser registrades al seu nom (atenent que es deriva d'un contracte de serveis licitats per l'Agència de Ciberseguretat de Catalunya).

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

Caldrà tenir en compte l'estratègia proposada pel licitador per assumir el control i la operació de totes les eines que li donaran suport en la execució del servei, atenent els criteris desenvolupats al present document. De manera general, es valorarà positivament l'ús de solucions "de mercat", posicionades en rankings estàndard dins del sector, com son Gartner o Forrester.

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

Aquest document inclou indicacions de com es pot accedir al llistat actualitzat d'eines específiques disponibles dins de l'Agència de Ciberseguretat de Catalunya.

4.7 GOVERN DE LA DADA I GOVERN DEL RISC

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

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

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

Aquests indicadors propis del servei, són proposats, desenvolupats, generats i mantinguts pel servei de suport i acordats amb el Responsable de la Funció d'Intel·ligència Operativa i

s'hauran de reportar periòdicament (com a molt en períodes mensuals) a aquest responsable per al seguiment del mateix.

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

El govern de tots aquests indicadors correspon a la funció de Gestió Operativa del SOC, i tant els indicadors de servei com els indicadors d'activitat s'hauran de reportar i processar amb les eines que indiqui l'Agència de Ciberseguretat de Catalunya (actualment l'eina interna desenvolupada internament INFOSOC i Confluence) i, si no es tracten directament amb dites eines, s'hauran de generar i processar amb eines compatibles amb les previstes per l'Agència de Ciberseguretat de Catalunya.

4.8 INFRAESTRUCTURA I EQUIPAMENT PER LA PRESTACIÓ DELS SERVEIS

L' Agència de Ciberseguretat de Catalunya, quan l'adjudicatari requereixi presencialitat física en les seves instal·lacions, proveirà:

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l' Agència de Ciberseguretat de Catalunya.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per a la prestació del servei a les instal·lacions escollides pel Agència de Ciberseguretat de Catalunya.
- Telefonia fixa a les instal·lacions del servei.
- 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.

L' Agència de Ciberseguretat de Catalunya no proveirà:

- Ordinadors de sobretaula, portàtils, tauletes amb sistema operatiu i programari.
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l' Agència de Ciberseguretat de Catalunya. Per tant cada tècnic te que disposar d'un mòbil que també serà emprat per doble factor d'autenticació.
- Accés a Internet via 4G/5G.
- Cap altre recurs no especificat explícitament.

En conseqüència, l'adjudicatari, quan requereixi presencialitat física a les instalacions de l'Agència de Ciberseguretat, haurà de:

- Subministrar tots els elements de maquinari, assumir el cost del llicenciament del programari i serveis, així com del seu manteniment, durant la durada del contracte,

que siguin necessaris per complir amb els requeriments d'aquest capítol. Aquests elements seran d'ús exclusiu pels serveis prestats a l' Agència de Ciberseguretat de Catalunya 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 pel servei de *Seguretat Corporativa* de l' Agència de Ciberseguretat de Catalunya.
- Permetre l'administració, maquetat i supervisió dels equips per part de l'equip de *Mitjans Tècnics* de l' Agència de Ciberseguretat de Catalunya.

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:

- Agència de Ciberseguretat de Catalunya decidirà la utilització de qualsevol tecnologia nova o evolució de les existents, relacionades amb la prestació del servei.
- Agència de Ciberseguretat de Catalunya 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 pe l' Agència de Ciberseguretat de Catalunya.

Es tindrà en consideració eines en els següents àmbits:

- Eines que facilitin la industrialització dels serveis (automatització, auto-aprovisionament, administració centralitzada, gestió/difusió del coneixement, etc.)
- Que les eines que s'integrin fàcilment amb les eines existents.
- El licitador ha de comptar amb el coneixement demostrable per la instal·lació, configuració, administració i operació de les eines que ofereixi, i haurà de transferir si fos necessari aquest coneixement a l'equip de Mitjans Tècnics encarregat de la seva administració i manteniment.

4.9 SEGURETAT CORPORATIVA

Tant l'empresa adjudicatària com el personal de l'adjudicatari s'haurà de sotmetre a les polítiques i regulacions internes que estableix el servei 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 de Ciberseguretat de Catalunya (sigui o no per l'exercici de la seva funció).

- Acceptar les normes i polítiques que estableix el servei 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 Enginyeria de Sistemes d'Informació 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 de Ciberseguretat de Catalunya.
- Garantir la 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 (GDPR, LOPD, LSSI, etc).

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

4.10 CONTROL DE GESTIÓ

El personal del licitador haurà de col·laborar amb l'àrea de Control de Gestió de l' Agència de Ciberseguretat de Catalunya per tal de:

- Definir un model de transparència en termes de capacitat i execució de tasques.
- Ajustar-se als procediments de facturació que determini l' Agència de Ciberseguretat de Catalunya.
- Conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència de Ciberseguretat de Catalunya, d'acord amb els procediments establerts.
- Exercir la gestió del contracte amb capacitats de forecast.
- Si aplica, realitzar el reporting en les eines proporcionades per l' Agència de Ciberseguretat de Catalunya 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.
    - Informes de servei mensual resum de l'activitat i del esforç aplicat .
- Memòria anual d'activitat .
- 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 de Ciberseguretat de Catalunya 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 de Ciberseguretat de Catalunya farà una notificació amb dues setmanes d'antelació.

L'adjudicatari suportarà els costos d'auditories adjudicades a tercers i gestionades per l'Agència de Ciberseguretat, destinant al seu finançament un màxim del 0.7% de l'import anual dels serveis contractats. En cas de no destinar-se la totalitat d'aquest import per a les finalitats d'auditoria, l' Agència de Ciberseguretat de Catalunya podrà demanar a l'adjudicatari l'execució d'altres tipus de serveis per valor de l'import no utilitzat.

4.11 PROPIETAT I VALIDACIÓ DE LA DOCUMENTACIÓ

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

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

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

4.12 INTEGRACIÓ AMB ALTRES EQUIPS

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

En aquest sentit, el SOC/CERT es relaciona en funció del model de relació establert per a cada funció i cada servei de suport, amb els següents actors:

Agència de Ciberseguretat de Catalunya:

- Serveis Corporatius
  - Comunicació i relacions institucionals
  - Assessoria jurídica
  - Administració i finances
  - Seguretat Corporativa

- Àrea de Govern del Risc
  - Governança de la seguretat (GVS)
  - Valoració del risc TIC (RIT)
  - Seguretat en el Disseny (SDI)
- Àrea de Compliment Normatiu.
  - Auditoria i marc normatiu (AMN)
  - Compliment regulatori (CRG)
- Àrea d'Estratègia de la seguretat
  - Anàlisi de tendències (ATS)
  - Internet segura (ITS)
- Centre d'Operació de la Seguretat
  - Evolució i Transformació (ETR)
  - Gestió Operativa (GES)
  - Mitjans Tècnics (MTC)
  - Control i Operació del Perímetre (COP)
  - Intel·ligència Operativa (IOP)
  - Resposta Activa (RAC)

CTTI

- Centre de Control
- Serveis d'operacions: CPD, NUS, Lloc de Treball, SAU
- Serveis de solucions: arquitectura corporativa, integració de solucions, S.I Transversals.
- Proveïdors de servei: CPD, Aplicacions, Comunicacions i Lloc de treball.

Clients

- Departaments i organismes de la Generalitat de Catalunya
- Administració Local
- Universitats i Centres de Recerca
- Hospitals
- Entitats del sector públic de la Generalitat
- Tercers

- Ciutadania.

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 de Ciberseguretat de Catalunya) com a nivell tàctic i estratègic.

L'adjudicatari haurà de plantejar a la seva proposta els models de relació que consideri oportuns, segons la seva visió de l'organització dels equips de treball que composen l'Agència de Ciberseguretat de Catalunya.

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

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

Caldrà detallar amb claredat el model de relació del servei de suport amb la resta d'actors amb els que ha de relacionar-se. Als serveis per els que no es requereix presencia física a les instal·lacions de l'Agència de Ciberseguretat, com es el cas d'Intel·ligència Operativa, es valorarà particularment la proposta per garantir una col·laboració plena, particularment entre totes les funcions del SOC/CERT, independentment de si la proposta del licitador inclou modalitat amb presencialitat física, completament remota o model híbrid.

4.13 INNOVACIÓ

En un mon tant canviant com és el de la ciberseguretat, es fonamental disposar d'una visió continuada en les diferents iniciatives, tant de caràcter tecnològic com de caràcter procedimental, d'innovació que puguin suposar una evolució i millora rellevant del SOC.

Per tot plegat, el licitador podrà incloure a la seva oferta propostes d'innovació que permetin la millora, evolució i industrialització dels serveis objecte de la present licitació, mitjançant el desplegament de solucions i processos capdavanters.

5 ACORDS DE NIVELL DE SERVEI I PENALITZACIONS

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

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

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

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

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

5.1 MODEL DE MESURA DEL NIVELL DE SERVEI

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

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

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

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

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

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

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

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

5.1.1.1 Bloc de servei Lot 1: Servei de suport de Resposta Activa

Codi	Nom	Descripció	Formula de cálcul / Eines	Periodicitat	Objetiu	ANS
OSGPE01	Efectivitat en la gestió de peticions	Volum de resolució de peticions, amb resultat satisfactori i en el termini segons la taula de prioritats	[%] (Peticions resoltes satisfactòriament (peticions no reobertes) en termini segons taula de prioritat) / (Total peticions resoltes)	Mensual	75%	95%
OSGPQ01	Qualitat dels lliurables del servei	Grau de satisfacció de l'Agència respecte dels lliurables. Es mesura la qualitat dels lliurables del servei, entre d'altres: informes, mètriques, indicadors	Puntuació de 1 (més satisfactori) a 6 (menys satisfactori) segons enquestes de satisfacció al responsable del servei per part de Agència de Ciberseguretat i/o el Director de l'Àrea.	Trimestral	5	3
OSGPQ02	Qualitat de la informació del servei	Manteniment i qualitat de la informació de suport del servei (diagrames, arquitectures, protocols d'actuació, instruccions operatives, descripció dels serveis, descripció dels processos, CMDB). Caldrà disposar d'un mapa documental que doni una visió global de la documentació rellevant del servei.	Puntuació de 1 (més satisfactori) a 6 (menys satisfactori) segons enquestes de satisfacció al responsable del servei per part de Agència de Ciberseguretat i/o el Director de l'Àrea.	Trimestral	5	3
OSGPP01	Compromís amb les dates d'entrega	Entrega dels lliurables del servei fora del temps acordat (informes, mètriques, indicadors, etc.)	Dies desviats respecte la data d'entrega establert	Per informe/ mètrica /indicador	10	1
OSGPP02	Compromís amb les dates d'execució de les actuacions	Volum de resolució satisfactoria en temps de les actuacions	Dies desviats respecte la data d'execució establerta	Per actuació	10	1
OSGPC01	Compliment amb les polítiques, normes i procediments	Incompliment dels procediments, protocols d'actuació o instruccions operatives del servei, així com amb qualsevol de los polítiques de seguretat de la Generalitat de Catalunya i/o de l'Agència.	En cas d'incompliment molt greu que provoqui un impacte important a l'Agència o als seus clients, s'aplicarà la penalització màxima. En cas contrari, si l'incompliment no és molt greu, es mesurarà la reiteració: Número d'incompliments de tipus greu o no greu.	Mensual	10	5
OSGI01	Gestió d'incidents de seguretat	Temps de primera resposta, temps que es triga des de la identificació/notificació de l'incident fins a la primera acció realitzada des del servei.	(%) Número de peticions amb una primera resposta en un temps inferior o igual al temps de catàleg (10 min)/número total de	Mensual	75%	95%

			les notificacions rebudes en el mes en curs			
OSGI03	Investigacions/ Gestió d'evidències	Temps de resposta en la gestió de l'incident in Situ i en el termini definit segons la següent taula de prioritat (adquisició d'evidències, gestió/suport, comité de crisi, etc.): Zona A: rati de 50 Km des de les oficines de l'Agència. *Critica < 1 hora *Alta < 1,30 hores *Normal < 4 hores *Baixa < 12 hores Zona B: rati de 100 Km des de les oficines de l'Agència. *Critica < 2 hores *Alta < 3 hores *Normal < 6 hores *Baixa < 12 hores Zona C: rati més de 100 Km des de les oficines de l'Agència. *Critica < 6 hores *Alta < 8 hores *Normal < 16 hores *Baixa < 24 hores	(%) Número d'incidents resolts a on hagi estat necessari realitzar accions in-Situ i la mitja del temps per donar-hi resposta hagi estat inferior o igual al temps establert en taula de prioritat / Número total d'incidents gestionats a on ha estat necessària a la intervenció in-Situ. Factor de penalització segons la ponderació de prioritat: * Crític: n=2 * Alt: n=1,75 * Normal: n=1,5 * Baix: n=1	Mensual	85%	98%
OSGI05	Extracció d'indicadors	Percentatge d'incidents a on s'ha extret la informació a nivell d'indicador vàlida per a la correlació i compartició amb tercers si fos necessari.	(%) Número d'incidents amb extracció d'indicadors necessaris per la compartició d'informació amb tercers / Número total d'incidents	Mensual	80%	98%

5.1.1.2 Bloc de servei Lot 2: Servei de suport d'Intel·ligència Operativa

Categoria	Nom	Descripció	Formula de càlcul / Eines	Periodicitat	Objectiu	ANS
Estratègia d' assoliment d' objectius	Desviament respecte a les fites definides a l'estratègia	Nombre d'objectius no assolits al període	**	Mensual	**	**
Gestió de demanda	Resposta Inicial	Percentatge mínim de peticions amb una primera resposta en un temps igual o inferior a l'objectiu	(Peticions amb resposta dins del temps / Total peticions) x100	Mensual	8h	90%

			Eina Ticketing			
	Peticions de serveis resoltes en termini	Percentatge mínim de peticions resoltes en un temps igual o inferior al temps acordat al catàleg de peticions de serveis del SOC/CERT*	(Peticions resoltes dins de temps / Total peticions) x100 Eina Ticketing	Mensual	100%	95%
	Disponibilitat del servei	Percentatge mínim de disponibilitat del servei	Tall de Servei - Ticketing	Mensual	100%	99,99%
	Satisfacció del Responsable del Servei	Grau mínim de satisfacció mitjana del RLS d'Intel·ligència Operativa i del RLS del Catalonia CERT	Suma (Grau de satisfacció RLS) / Nombre de RLS avaluats	Mensual	100%	80%
Pronòstic i investigació de ciberamenaces	Intel·ligència accionable disponible	Percentatge mínim d'amenaces dins del pronòstic d'amenaces que inclouen Intel·ligència associada per permetre la prevenció i la resposta	(Nombre ciberamenaces al pronòstic amb Intel·ligència associada / Total ciberamenaces al pronòstic) x100	Mensual	100%	90%
Estratègies de resposta	Millora continua de les estratègies	Percentatge mínim d'estratègies actualitzades després d'identificar millores requerides, durant la gestió d'una crisis.	(Nombre d'estratègies actualitzades després d'identificar millores durant la gestió d'una crisis) / Total estratègies que requereixen millores segons les conclusions de la gestió d'una crisis) x100	Mensual	100%	90%
Orquestració i context	Crisis gestionades amb estratègia	Percentatge mínim d'amenaces, incidents i atacs **greus** gestionats a partir d'una estratègia de resposta prèviament existent i activament validada.	(Nombre de crisis gestionades a partir d'una estratègia validada / Total crisis gestionades) x100	Mensual	100%	80%
	Context operatiu disponible	Percentatge mínim d'esdeveniments de context rellevants per l'operació comunicats als equips del SOC/CERT	(Nombre d'esdeveniments de context reportats al SOC/CERT / Total d'esdeveniments de context) x100	Mensual	100%	80%

* A títol informatiu, actualment els temps de resolució de serveis com el de Càlcul del grau d'exposició a l'amenaça estan pendents de fixar i haurà de ser el propi servei el que colabori en la seva definició.

** Segons la estratègia d'assoliment d'objectius de l'adjudicatari. **Cada incompliment d'un objectiu definit en aquesta estratègia es computarà com a un incompliment d'un Acord de Nivell de Servei independent**.

De l'anterior taula s'ha de tenir en compte que l'indicador amb nom "Incompliment d'objectius" pot comportar, a efectes de càlcul de penalitzacions, l'incompliment de més d'un acord de nivell de servei de manera simultània. En incomplir per exemple dos objectius, segons la estratègia d'assoliment proposada per l'adjudicatari, es computarà com a dos incompliments independents dels Acords de Nivell de Servei (ANS).

L'Agència de Ciberseguretat verificarà els ANS i aixecarà acta que signaran el responsable del contracte de l'empresa adjudicatària i el responsable del contracte per part de l'Agència de Ciberseguretat.

5.1.2 Modificació dels indicadors i nivells de servei

Al llarg de la prestació del servei, davant qualsevol modificació dels indicadors i nivells de servei, amb l'objectiu de donar un millor servei, l'Agència de Ciberseguretat, conjuntament amb el proveïdor, consensuaran i planificaran la seva introducció.

Algunes de les causes que poden comportar aquestes modificacions són: les variacions d'entorn tecnològic, els canvis d'abast i volum, les innovacions i les millores dels propis serveis.

5.2 MODEL DE PENALITZACIONS

L'adjudicatari del contracte està obligat al compliment del termini total d'execució del contracte i dels terminis parcials establerts en aquest. Si en relació amb qualsevol termini dels establerts en el contracte, l'adjudicatari incorre en una demora per causes imputables a ell, l'Agència podrà optar per la resolució del contracte.

L'Agència de Ciberseguretat tindrà la facultat, respecte a l'incompliment per causes imputables a l'adjudicatari de l'execució parcial o insatisfactòria dels serveis i les prestacions definides en el contracte, d'aplicar les penalitzacions definides en aquest apartat.

Els acords de nivell de servei (ANS) que haurà de complir l'adjudicatari seran els que el licitador proposi dins de la seva oferta, que hauran de ser com a mínim els indicats en aquest capítol però podran ser millorats, i un cop s'hagin validat i acordat amb l'Agència després de la signatura del contracte.

5.2.1 Càlcul de les penalitzacions

A continuació descrivim el model de penalitzacions que s'aplicaran per l'incompliment dels Acords de nivell de servei (ANS) d'acord amb els criteris, quantificació i mètode de càlcul establerts, al qual s'haurà d'ajustar el licitador.

Cada mes, trimestre i semestre es calcularan els valors resultants dels diferents ANS, analitzant quants d'ells compleixen amb els valors definits. El nombre d'indicadors que no assoleixin els valors objectius (SLO), definiran el valor d'incompliment del període, que podrà ser: *lleu, greu, o molt greu*.

El percentatge de penalització corresponent a aplicar sobre l'import mensual de la factura serà el que s'obté de la següent taula:

TIPUS D'INCOMPLIMENT	Núm. de SLO incomplert/Període	Descompte Aplicable
Lleu	**2 SLO incomplerts**	**3% de l'import de la Factura**
Greu	**3-4 SLO incomplerts**	**5% de l'import de la Factura**
Molt greu	**>= 5 SLO incomplerts**	**10% de l'import de la Factura**

5.2.2 Aplicació de les penalitzacions

L' Agència de Ciberseguretat de Catalunya té la potestat de decidir aplicar les penalitzacions econòmiques o bé les compensacions en serveis equivalents.

L' Agència de Ciberseguretat de Catalunya té la potestat de decidir no aplicar les penalitzacions associades per l'incompliment dels nivells de servei acordats en determinades casuístiques. Com a regla general queden excloses les penalitzacions quan:

- Existeixin situacions extraordinàries que donin lloc a alteracions que desvirtuïn la mesura.

- Quan es produeixi una situació excepcional d'un increment dràstic de l'activitat, no atribuïble a l'adjudicatari que impedeixi l'assoliment dels ANS acordats.
- Quan la desviació sigui provocada per components que no estan sota la responsabilitat de l'adjudicatari.
- Quan el servei quedi aturat per causes alienes al mateix servei, siguin aturades programades o no.

A l'inici del contracte, l'adjudicatari podrà sol·licitar a l' Agència de Ciberseguretat de Catalunya la revisió temporal i transitòria de les penalitzacions sobre els ANS que cregui necessàries en atenció a elements de caràcter extraordinari. L' Agència de Ciberseguretat de Catalunya estudiarà la seva viabilitat i/o aplicació i les aprovarà per escrit, si s'escau.

5.2.3 Incidències en les mesures d'Indicadors

En cas d'incidències en la mesura del valor d'un Indicador associat a un ANS degudes a errors materials, o quan existeixi manca de col·laboració per part de l'adjudicatari en la determinació del valor correcte, es considerarà que l'indicador no ha arribat al nivell mínim de servei, aplicant-se la penalització corresponent.

Es considerarà que hi ha incidència en la mesura d'un indicador quan el valor d'aquest, facilitat per l'adjudicatari difereixi en més d'un 15% respecte del valor real auditat que resulti del procés d'auditoria que es descriu al Document tècnic de solució final.

Es considerarà manca de col·laboració quan conflueixin tots els següents factors:

- Que l'auditor que es designi en l'esmentat procés d'auditoria aporti evidència d'una sol·licitud d'informació en un termini concret dirigida a l'adjudicatari.
- Que la sol·licitud d'informació demanada i el termini siguin raonables a judici de l' Agència de Ciberseguretat de Catalunya.
- Que l'adjudicatari no pugui aportar cap evidència que provi que s'hagi facilitat la informació demanada dins del termini especificat o en el seu defecte no hagi donat una explicació raonable del motiu del retard.

5.2.4 Facturació de les penalitzacions

L'import corresponent a les penalitzacions aplicades a l'adjudicatari és resultat de sumar els imports de penalització corresponents a l'incompliment dels nivells de serveis acordats en el contracte.

L'adjudicatari abonarà, mitjançant el procediment de compensació, les penalitzacions automàticament a la factura que pels seus serveis hagi d'abonar l' Agència de Ciberseguretat de Catalunya. En cas de no poder compensar-se els imports per causes imputables a l'adjudicatari aquest haurà de satisfer l'import mitjançant el pagament corresponent a l' Agència de Ciberseguretat de Catalunya.

La no incorporació d'aquesta reducció de l'import per qualsevol causa (tramitació, incidència en terminis de facturació, etc.) no eximirà a l'adjudicatari de la seva obligació de pagament en els termes que determini l' Agència de Ciberseguretat de Catalunya.

5.2.5 Incompliment de la normativa interna de l' Agència de Ciberseguretat de Catalunya

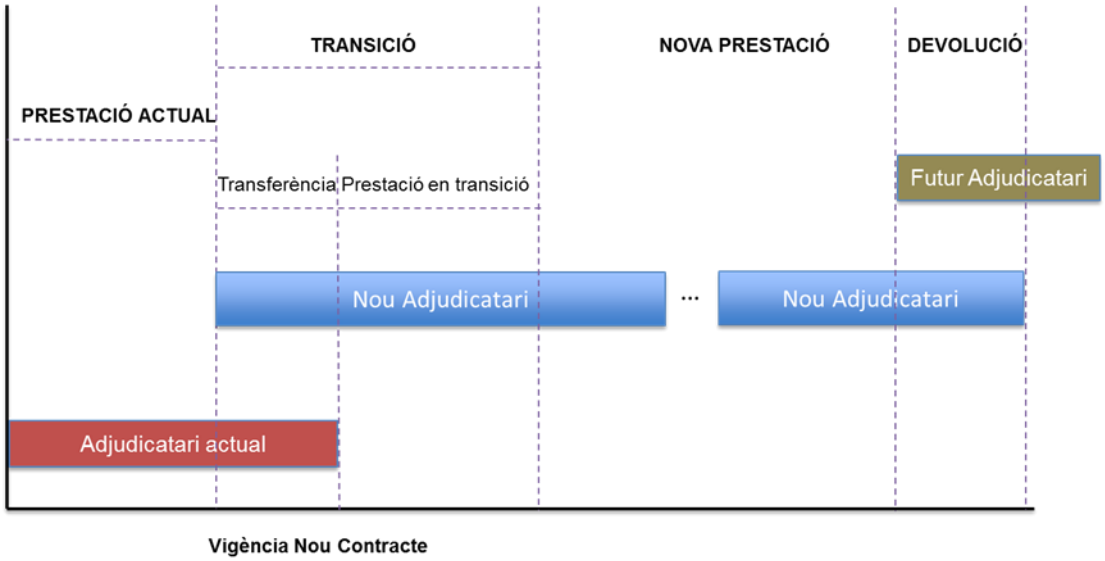
Tal com s'ha exposat a l'apartat de Seguretat Corporativa del present plec l' Agència de Ciberseguretat de Catalunya disposa de normativa reguladora en matèria de seguretat corporativa i de protecció de la seva informació. L'incompliment d'aquesta normativa pot implicar greus perjudicis a l' Agència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

L' Agència de Ciberseguretat de Catalunya aplicarà una penalització per un import d'entre el 10 i el 30% del cost mensual del servei, per un incompliment clar respecte a la normativa vigent en matèria de seguretat corporativa i normativa interna que realitzi l'adjudicatari i el personal que aquest aporti (incloent-hi el personal que pugui aportar en subcontractacions sota la seva responsabilitat). La graduació de l'import es produirà, atenent la gravetat, continuïtat de la infracció, duració, intensitat, grau de risc que hagi causat la infracció, entre d'altres. En cap cas aquesta penalització limitarà la capacitat de l'Agència de Ciberseguretat de Catalunya de reclamar els danys i perjudicis efectivament causats per l'incompliment d'acord amb el contracte vigent entre les parts.

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

6 FASES DE LA PRESTACIÓ

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



Fases de la prestació

6.1 TRANSICIÓ

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

Durant la transició es duran a terme les següents activitats:

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

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

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

  A l'Agència de Ciberseguretat de Catalunya se li deurà presentar un *checklist* de les solucions i/o tecnologies conforme han estat correctament traspassades. La

seguretat, com no pot ser d'una altre manera, es un eix principal, per tant tots els elements relacionats amb la seguretat deuran de tindre especial atenció amb aquest *check*.

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

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

  Aquesta fase podrà ser modificada en funció al resultat de l'anàlisi a lliurar al final de la transferència i el pla d'acció que s'estableixi.

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

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

6.2 NOVA PRESTACIÓ

Es considera la fase normal de la prestació del servei. Comença quan els processos de transició hagin acabat fins 1 mes abans que finalitzi la prestació del servei.

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

6.3 DEVOLUCIÓ

Fase que s'emmarca al final de la prestació, un cop s'hagi comunicat la cancel·lació del contracte, **un mes** abans de l'extinció d'aquest. Durant aquest mes hi haurà coexistència amb un nou adjudicatari fins que es transfereixen els serveis a aquest.

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

Tot el material desenvolupat, incloent-hi desenvolupaments en Sistemes d'Informació, és propietat de l' Agència de Ciberseguretat de Catalunya i romandrà, amb tota la seva

documentació, en l' Agència de Ciberseguretat de Catalunya un cop acabada la prestació del servei.

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

Tal com s'ha descrit a la secció d'eines i equipament per a la prestació, els Enginyeria de Sistemes d'Informació que el proveïdor sortint hagi proporcionat per tal de desenvolupar la seva tasca hauran de ser degudament esborrats i tota la informació traspassada a qui l' Agència de Ciberseguretat de Catalunya designi.

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

7 ANNEX I – LLISTAT D'EINES

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

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

8 MARC NORMATIU

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

- GUIT007-C - Protecció entorns Linux
- GUIT061-C - Protecció entorns Windows Server 2012
- GUIT063-C - Protecció entorns SQL Server 2012
- GUIT064-C - Protecció entorns Microsoft SharePoint 2013
- GUIT073-C - Protecció entorns Windows 7 i 8
- GUIT074-C - Protecció entorns MySQL 5x
- NOR0018-C - Norma de mesures de seguretat en la construcció de sistemes informació
- GUIT019-C - Guia de contrasenyes
- GUIT020-C - Gestió de comptes administració de sistemes
- GUIT044-C - Guia eliminació segura informació en la reutilització o destrucció de suports i sistemes
- PRC0001- C - Procediment de notificació d'incidents de seguretat
- GUIT023-C - Guia de seguretat física de CPDs i sales tècniques
- GUIT040-C - Guia de còpies de seguretat
- GUIT050-C - Guia de gestió de la continuïtat del negoci
- GUIT065-C - Trasllat de CPDs i migració de dades
- GUIT002-C - Guia d'administració del correu electrònic
- GUIT003-C - Guia d'administració de l'estació de treball
- GUIT004-C - Guia d'administració de xarxes WiFi
- NOR0016-C - Gestió de traces
- NOR0046-C - Navegació Web de la Generalitat de Catalunya
- FRM0004-C - Memòria del sistema de videovigilància
- FRM0008-C - Document d'acceptació d'obligacions relatives a seguretat de la informació i protecció de dades de caràcter personal
- GUIL071-C - Guia Legal Seguretat ENS Metodologia
- NOR0003-C - Contractació de Tercers
- GUIT026-C - Ús del correu electrònic

- NOR0005-C - Contrasenyes
- PRT0009-C - Model de protocol sobre l'ús de dispositius no corporatius
- Nota en relació amb l'ús de serveis disponibles a la xarxa que permeten compartició de fitxers i d'altres

A L'Hospitalet de Llobregat, en la data indicada

Alex Novella
Responsable Línia de Servei de detecció i prevenció d'amenaces

Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya

www.ciberseguretat.cat