Agència de Ciberseguretat de Catalunya

PLEC DE PRESCRIPCIONS TÈCNIQUES

Serveis per a la monitorització del nivell de ciberseguretat de Catalunya i la implementació de l'Índex de Ciberseguretat

LOT 1. Servei per al càlcul del nivell de ciberseguretat a Catalunya a través de la recollida i anàlisi massiu d'evidències

LOT 2. Disseny, desenvolupament, implantació, posada en servei i manteniment de l'Índex de Ciberseguretat de Catalunya

NÚM. EXPEDIENT CO.05.2020

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

ÍNDEX

1 Introducció

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència), té la necessitat de licitar un conjunt de solucions de suport per a l'execució de les funcions de seguretat TIC en virtut del "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 dels seus clients, l'Agència necessita dotar-se de les millors pràctiques, eines i proveïdors, per portar a terme els seus serveis, i entre ells, els Serveis de Suport en Ciberseguretat de l'Àrea d'Estratègia de la Seguretat amb l'objectiu de poder donar resposta als requeriments i encàrrecs rebuts.

1.1 L'Agència de Ciberseguretat de Catalunya

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

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

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

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

L'Agència com a encarregada d'establir i de liderar el servei públic de ciberseguretat, té com a objectiu garantir una Societat de la Informació segura i confiable per al conjunt de la ciutadania catalana i de la seva Administració Pública, amb la voluntat d'esdevenir un referent a nivell nacional i internacional en matèria de ciberseguretat.

Com a organisme competent en matèria de ciberseguretat, l'Agència es responsabilitza de l'establiment i el seguiment dels programes d'actuació en matèria de ciberseguretat, sota la direcció estratègica del Govern de la Generalitat de Catalunya, en coordinació amb les entitats del sector públic de l'Administració de la Generalitat de Catalunya, i col·laborant amb governs locals de Catalunya, sector privat i societat civil.

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

1.2 Context del servei

El servei a licitar es desenvolupa des de l'Àrea d'Estratègia de la Seguretat (en endavant, ESG) de l'Agència de Ciberseguretat, que té la missió de vetllar per l'alineament dels productes i serveis de l'Agència amb les experiències internacionals de referència. A nivell operatiu, aquesta àrea realitza un anàlisi de les tendències en l'àmbit de la ciberseguretat per tal d'extreure conclusions en matèria de les ciberamenaces relacionades amb la Generalitat de Catalunya i l'Administració pública local per tal de desenvolupar els Programes de Seguretat dels Departaments i el Programa d'Internet Segura de la Generalitat de Catalunya.

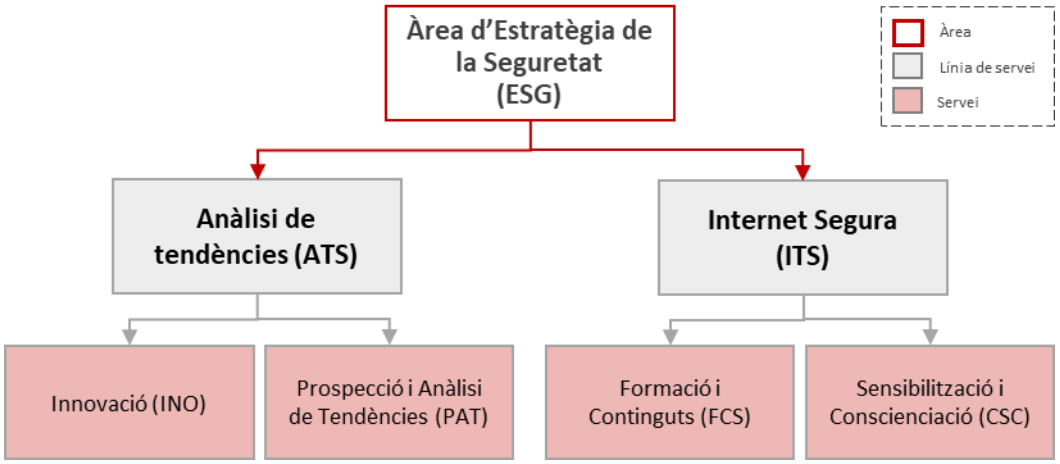
L'àrea ESG s'estructura en dues línies de servei que s'interrelacionen i es complementen per tal de garantir el correcte desenvolupament de les funcions de l'àrea i les seves corresponents funcions es detallen a continuació.

— La línia de servei d'Anàlisi de Tendències de Seguretat (en endavant, ATS) es divideix en els serveis d'Innovació (en endavant, INO) i de Prospecció i Anàlisi de Tendències (en endavant, PAT). Té els objectius de:

  - Capacitar l'entitat com una font d'opinió i posicionament enfront l'evolució i les tendències que puguin succeir en l'àmbit de la ciberseguretat a nivell del sector,
  - Anàlisi continu de la informació i activitat rellevant recollida de fonts internes i d'arreu del món amb l'objectiu de generar indicadors de seguretat per identificar tendències.
  - Preveure possibles futurs incidents a curt termini i alinear els programes de Seguretat a mig termini.
  - Promoció de plans i iniciatives innovadores en matèria de ciberseguretat.

— La línia de servei d'Internet Segura (en endavant, ITS) es divideix en els serveis de Formació i Continguts (en endavant, FCS) i Sensibilització i Conscienciació (en endavant, CSC). Té els objectius de:

  - Gestió de diferents modalitats de formació per a les administracions públiques catalanes.
  - Elaboració de diversos continguts de conscienciació, en l'àmbit de la formació presencial i formació virtual.
  - Elaboració de materials de sensibilització que es difonen a través de diferents accions multicanal (xarxes socials i web pròpies i de tercers).
  - Preparació de monogràfics i campanyes de sensibilització anuals (Dia d'Internet Segura o el Mes Europeu de la Ciberseguretat a Catalunya, campanyes d'hàbits cibersaludables, campanya per a empreses, etc.).



Organització de les línies de servei i serveis de l'àrea d'Estratègia de la Seguretat (ESG)

Les ciberamenaces estan darrere dels principals riscos de la societat del segle XXI, cada vegada més interconnectada, globalitzada, canviant i complexa, i esdevé imprescindible avançar-se a les seves causes i preveure'n les conseqüències. La ràpida evolució de les ciberamenaces requereix un control exhaustiu i continuat de l'exposició del perímetre dels sistemes d'informació de l'Administració pública així com del territori de Catalunya en general, ja sigui monitorant els atacs, com analitzant les vulnerabilitats existents, amb l'objectiu de disposar d'una avaluació objectiva de l'estat del nivell de maduresa en matèria de ciberseguretat. A partir de la qualificació del nivell de ciberseguretat, serà possible adquirir capacitació per al control i la investigació dels riscos, planificar programes de mitigació i la creació d'un espai de col·laboració, en el qual es puguin compartir les troballes de ciberseguretat i fer-ne un seguiment mitjançant indicadors clau per fomentar una acció ràpida i efectiva.

Per tal de dur a terme aquest servei de forma adequada es requereixen capacitats expertes, d'una banda, en l'anàlisi de les xarxes de comunicacions electròniques i dels sistemes d'informació del territori de Catalunya i, d'altra banda, en el disseny, desenvolupament, implantació, posada en servei i manteniment d'un sistema d'informació per a la ingesta, emmagatzematge, càlcul i visualització d'indicadors en matèria de ciberseguretat que prendrà la forma de l'Índex de Ciberseguretat de Catalunya.

1.3 Estructura dels lots

Amb l'objectiu de facilitar l'especialització de les activitats requerides de la licitació emmarcada en el present lot, aquesta queda separada en dos lots, cadascun dels quals requereix un conjunt d'activitats diferenciades per a les quals els licitadors han de preparar una oferta específica.

— **LOT 1. Servei per al càlcul del nivell de ciberseguretat a Catalunya a través de la recollida i anàlisi massiu d'evidències**

Es requereix una solució que, a partir de la recollida massiva d'evidències d'Internet vinculades a diferents factors representatius de la ciberseguretat (com els ciberatacs per infecció amb *malware* o les vulnerabilitats), calculi el nivell de ciberseguretat de la infraestructura de la Generalitat de Catalunya sota supervisió de l'Agència i de tot el territori de Catalunya. El càlcul d'aquest nivell de ciberseguretat ha de ser continuat en el temps i basat en un algoritme objectiu a partir d'un conjunt d'indicadors acurats i en un

nombre suficient d'evidències amb l'objectiu de garantir la seva qualitat i fiabilitat. La solució ha de permetre la monitorització continuada del nivell de ciberseguretat i, a més, facilitar que les evidències, mètriques i indicadors obtinguts alimentin de forma automatitzada l'Índex de Ciberseguretat (Lot 2).

— **LOT 2. Disseny, desenvolupament, implantació, posada en servei i manteniment de l'Índex de Ciberseguretat de Catalunya**

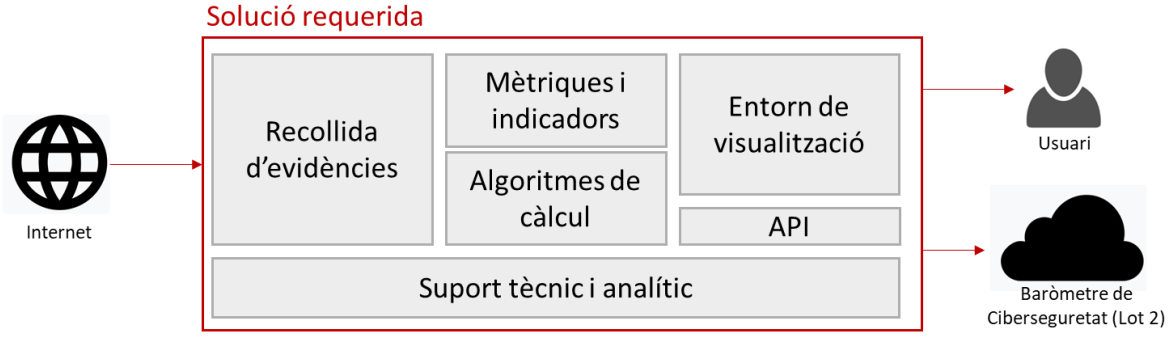
Es requereix un servei que dissenyi, desenvolupi, implanti, posi en servei i mantingui un sistema d'informació on s'aglutini, es processi i s'emmagatzemi estructuradament la informació provinent de diferents fonts, en múltiples formats i suports, amb l'objectiu de visualitzar un conjunt d'indicadors que descriguin, de forma entenedora, les característiques i evolució de les tendències en matèria de ciberseguretat a Catalunya de manera que ofereixi suport a l'acció estratègica de l'Agència a tots els nivells. La solució desenvolupada ha de recollir les evidències, mètriques i indicadors de generats des de la solució per al càlcul del nivell de ciberseguretat a Catalunya a través de la recollida i anàlisi massiu d'evidències (Lot 1).

2 LOT 1: SERVEI PER A LA MONITORITZACIÓ DE LA CIBERSEGURETAT A CATALUNYA

2.1 Objecte

La ràpida evolució de les ciberamenaces requereix un control exhaustiu i continuat de l'exposició del perímetre dels sistemes d'informació. En aquest sentit, es requereix una solució que, a partir de la recollida massiva d'evidències d'Internet vinculades a diferents factors representatius de la ciberseguretat (com els ciberatacs per infecció amb *malware* o les vulnerabilitats), calculi el nivell de ciberseguretat de la infraestructura de la Generalitat de Catalunya sota supervisió de l'Agència i de tot el territori de Catalunya.

El càlcul d'aquest nivell de ciberseguretat ha de ser continuat en el temps i basat en un algoritme objectiu a partir d'un conjunt d'indicadors acurats i en un nombre suficient d'evidències amb l'objectiu de garantir la seva qualitat i fiabilitat. La solució ha de permetre la monitorització continuada del nivell de ciberseguretat i, a més, facilitar que les evidències, mètriques i indicadors obtinguts alimentin de forma automatitzada l'Índex de Ciberseguretat (Lot 2).



Esquema conceptual de la integració del servei del Lot 1

2.2 Abast

La licitació requereix la monitorització del nivell de ciberseguretat en tres nivells diferents:

- Global de Catalunya, dins les competències de l'Agència i en l'àmbit en el qual desplega les seves funcions.
- Sector públic Generalitat de Catalunya.
- Qualssevol altres entitats.

Per a cadascun dels àmbits, es requerirà la mesura del nivell de ciberseguretat i la corresponent recollida de les evidències i la generació d'indicadors que serveixen pel seu càlcul, de forma continuada i referenciada en el temps, i amb la classificació per sectors d'activitat.

2.3 Objectius del Servei

Els objectius de la present licitació són:

- Obtenir un sistema d'avaluació objectiva de l'estat del nivell de maduresa en matèria de ciberseguretat per a la Generalitat de Catalunya i la totalitat del territori de Catalunya.
- Obtenir les evidències i els indicadors necessaris, de forma continuada en el temps, per a l'anàlisi dels fenòmens actuals i les tendències en l'ús de les TIC per tal de determinar riscos i oportunitats de millora, tant a nivell de la Generalitat de Catalunya com en la totalitat del territori de Catalunya.
- Monitoritzar els incidents de seguretat a temps real i en base a les evidències recollides que tinguin lloc en l'àmbit dels sistemes d'informació connectats a Internet de la Generalitat de Catalunya i la totalitat del territori de Catalunya.
- Disposar de mètriques i indicadors basats en evidències necessaris per avaluar l'impacte de les accions endegades (plans de comunicació i conscienciació) sobre el nivell de maduresa en matèria de ciberseguretat a la Generalitat de Catalunya i la totalitat del territori de Catalunya.
- Disposar d'informació adient amb l'objectiu d'informar al Govern de les dades en matèria de ciberseguretat relatives a les entitats que gestionen serveis públics o essencials a Catalunya.
- Disposar d'un canal de comunicació per a la compartició amb l'Índex de Ciberseguretat (Lot 2), de forma automatitzada i periòdica, de les troballes en matèria d'evidències i indicadors recollits en l'àmbit de la Generalitat de Catalunya i de la totalitat del territori de Catalunya.

2.4 Requeriments tècnics

A continuació es descriuen els serveis, característiques i requisits que conformen l'objecte del contracte i que el licitador haurà d'ofertar. Es tracta d'uns requeriments mínims i necessaris, de manera que els licitadors podran ampliar-los i enriquir-los en les seves ofertes amb l'objectiu d'aspirar a una millora positiva en la valoració de l'oferta tècnica.

2.4.1 Visibilitat de la ciberseguretat de Catalunya

La solució proposada ha de dotar l'Agència amb la capacitat necessària per mesurar el nivell de maduresa en matèria de ciberseguretat a la totalitat del territori de Catalunya, entenent per això la valoració objectiva de l'estat de la seguretat de les seves xarxes de comunicacions electròniques i sistemes d'informació.

2.4.1.1 Càlcul del nivell de ciberseguretat de Catalunya

La solució proposada ha de calcular un indicador que representi el nivell de maduresa en matèria de ciberseguretat de tota Catalunya. Les característiques d'aquest indicador han de ser les següents:

- S'ha d'actualitzar amb una periodicitat mínima diària.
- Ha d'estar calculat de forma objectiva a partir d'un algoritme a partir d'un conjunt de factors basats en evidències (veure annex I).
- Ha de conservar un històric tant del conjunt de dades del nivell de ciberseguretat com les evidències per un període d'antiguitat mínim d'1 mes.
- Ha de possibilitar la comparativa amb un mínim de 5 països o territoris de naturalesa similar a Catalunya.
- Ha de classificar i permetre distingir el nivell de ciberseguretat i les evidències per sectors econòmics.

2.4.1.2 Provisió d'evidències d'incidents a temps real

La solució proposada haurà de disposar d'un mitjà per a l'obtenció o consulta de les evidències relatives a incidents de ciberseguretat ocorregudes dins del territori de Catalunya en temps real. Aquestes evidències monitoritzades de forma continuada en el temps són les que s'utilitzaran per al càlcul del nivell de maduresa en ciberseguretat i altres indicadors per al conjunt del territori.

2.4.1.3 Evidències per a Catalunya

Les evidències recollides han de ser objectives, representatives i se n'ha de disposar el nombre suficient per tal que l'aplicació de l'algoritme proposat pel licitador permeti obtenir l'indicador del nivell de maduresa en matèria ciberseguretat a Catalunya. Aquestes evidències han de permetre obtenir, com a mínim, les mètriques relatives a les categories d'incidents de seguretat que s'especifiquen en l'annex I.

2.4.2 Visibilitat de la ciberseguretat de la Generalitat de Catalunya

La solució proposada ha de permetre a l'Agència monitoritzar la ciberseguretat de la infraestructura tecnològica de la Generalitat de Catalunya i el seu sector públic, àmbits pels quals té la funció de planificar, gestionar, coordinar i supervisar la ciberseguretat.

2.4.2.1 Càlcul del nivell de ciberseguretat a la Generalitat de Catalunya

La solució proposada ha de calcular un indicador que representi el nivell de maduresa en matèria de ciberseguretat per a tota la infraestructura tecnològica de la Generalitat de Catalunya. Les seves característiques han de ser les següents:

- S'ha d'actualitzar amb una periodicitat mínima diària.

- Ha d'estar calculat de forma objectiva a partir d'un algoritme a partir d'un conjunt de factors basats en evidències (veure annex I).
- Ha de conservar un històric tant del conjunt de dades del nivell de ciberseguretat com les evidències per un període d'antiguitat mínim de 12 mesos.
- Ha de possibilitar la comparativa amb un mínim de 5 organitzacions de naturalesa similar a la Generalitat de Catalunya.

2.4.2.2 Evidències per la Generalitat de Catalunya

Les evidències recollides han de ser objectives, representatives i se n'ha de disposar el nombre suficient per tal que l'aplicació de l'algoritme proposat pel licitador permeti obtenir l'indicador del nivell de maduresa en matèria ciberseguretat per a la Generalitat de Catalunya. Aquestes evidències han de permetre obtenir, com a mínim, les mètriques relatives a les categories d'incidents de seguretat que s'especifiquen en l'annex I.

Addicionalment, ha de permetre obtenir el càlcul del nivell de maduresa en matèria de ciberseguretat i les mètriques relatives categories d'incidents per a entitats o agrupacions de xarxa de nivell inferior a la Generalitat de Catalunya (p. ex. les IP corresponents a una àrea específica).

2.4.3 Visibilitat de la ciberseguretat d'altres entitats

De forma anàloga a allò indicat per la Generalitat de Catalunya (2.4.2), la solució ha de permetre a l'Agència monitoritzar la ciberseguretat d'entitats específiques dins del seu àmbit d'interès competencial. S'hauran d'oferir les característiques següents:

- L'accés a la informació del nivell de maduresa en matèria de ciberseguretat, indicadors i evidències ha de ser accessible, de forma restringida, pels usuaris de l'entitat monitoritzada que l'Agència determini.
- S'ha d'actualitzar amb una periodicitat mínima diària.
- Ha d'estar calculat de forma objectiva a partir d'un algoritme a partir d'un conjunt de factors basats en evidències (veure annex I).
- Ha de conservar un històric tant del conjunt de dades del nivell de ciberseguretat com les evidències per un període d'antiguitat mínim de 12 mesos.
- Ha de possibilitar la comparativa entre organitzacions.
- Ha de permetre l'agrupació d'organitzacions similars per a la creació d'agrupacions de naturalesa similar.

Els licitadors hauran d'incloure en la seva oferta, com a mínim, la possibilitat d'obtenir la visibilitat sobre un total de 100 entitats. Addicionalment, hauran d'oferir la possibilitat d'analitzar el nivell de seguretat durant un període mínim limitat d'un mes per a un mínim de 10 entitats addicionals.

2.4.4 Integració amb l'Índex de Ciberseguretat

La solució ha d'oferir una API (*Application Programming Interface*) d'accés restringit per a l'Agència que habiliti, de forma segura, la transferència de qualsevol informació recollida per la solució cap al sistema d'informació de l'Índex de Ciberseguretat (Lot 2). Les consultes realitzades a través de l'API permetran capturar els indicadors del nivell de maduresa en matèria de ciberseguretat, les evidències recollides i les seves mètriques per a qualsevol període dins de l'històric de dades disponible.

2.4.5 *Reporting* interactiu: indicadors, informes i alertes

La solució proposada disposarà de diferents funcionalitats que permetran la consulta d'informació sota demanda:

- Quadres de comandament representatius dels indicadors actuals i històrics pel nivell de maduresa en matèria de ciberseguretat, per a les categories d'evidències recollides. Aquest *reporting* es podrà obtenir, a nivell del conjunt del territori de Catalunya i per a les entitats monitoritzades, classificables per sectors econòmics.
- Informes automàtics de diferent tipologia, executiva o extensa (en funció de si inclouen el detall de les evidències recollides o no), amb els indicadors actuals i històrics pel nivell de maduresa en ciberseguretat actual i pels indicadors de les categories d'evidències recollides. Aquest *reporting* es podrà obtenir, a nivell del conjunt del territori de Catalunya i per a les entitats monitoritzades, classificables per sectors econòmics.
- Alertes configurables que notifiquin sobre variacions, ja sigui increments o caigudes, del nivell de ciberseguretat, o sobre les evidències recollides.

2.5 Lliurable: informe executiu anual

Amb una periodicitat anual, l'adjudicatari prepararà un informe del nivell de maduresa en matèria de ciberseguretat per a Catalunya. S'hi inclourà el significat de les dades i la interpretació dels valors i tendències més rellevants. Aquest informe serà adequat, en qualitat i forma, per a la realització de presentacions executives davant de comitès de direcció i govern.

En aquest informe s'inclouran totes les tasques realitzades i els serveis implementats en el marc d'execució del contracte.

2.6 Suport

L'Agència requereix d'un conjunt de capacitats destinades a oferir suport funcional i resposta davant d'incidències que permetin optimitzar l'aprofitament exhaustiu de la solució.

- Eina de *ticketing* per a la gestió i de peticions i comunicació d'incidències.
- L'adjudicatari haurà de gestionar i resoldre les incidències ocorregudes relatives a tot allò que impliqui un funcionament incorrecte de la solució d'acord amb els ANS (2.11).
- L'adjudicatari haurà de resoldre aquelles consultes relacionades amb l'ús, l'administració o la configuració de la solució d'acord amb els ANS (2.11).
- L'adjudicatari mantindrà actualitzada la documentació relativa als procediments per a l'ús i configuració de la solució, així com per a l'API dedicada a la transferència de dades a l'Índex de Ciberseguretat.
- El suport haurà d'estar disponible en un horari de 8x5 dins de l'horari d'oficina de l'Agència.
- L'adjudicatari disposarà d'un equip per al suport analític expert que prestarà suport puntual a l'Agència en quant a l'anàlisi i interpretació dels canvis en el nivell de maduresa en matèria de ciberseguretat o de la informació recollida en les evidències i els indicadors.

2.7 Equip de suport

Es requereix un equip de persones destinat garantir el desenvolupament satisfactori del servei i la correcte consecució dels requeriments estipulats en el present plec, així com dotar de suport en l'ús de la solució i posar a disposició de l'Agència un suport analític expert. La seva dedicació estarà supeditada a les necessitats puntuals de l'Agència i no es requereix una dedicació total i exclusiva en cap cas.

Per tal de donar resposta a les activitats i productes descrits, l'àrea d'ESG requereix la incorporació dels recursos i perfils que s'assenyalen al quadre resum de característiques del PCAP i que constitueixen la solvència mínima requerida.

2.8 Fases de la prestació del Servei

Els licitadors hauran de presentar, dins la seva oferta tècnica, el pla d'actuació detallat per tal d'aconseguir una transició que asseguri la transferència de coneixement més adequada per en la devolució del servei a la seva finalització.

2.8.1 Inici

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

El servei de la present licitació és nou i no en substitueix cap. Amb l'objectiu d'aconseguir un inici eficient, cal assegurar que es duran a terme les següents activitats:

- Reunió d'inici per a la posta en marxa del servei.
- Establiment i ajust, si s'escau, de la planificació proposada per l'adjudicatari
- Lliurament de credencials i llicència, o en el seu defecte qualsevol dels recursos necessaris, amb l'objectiu de tenir accés al servei.
- Transferència de coneixement del funcionament del servei, les particularitats i de les millors pràctiques, de manera que l'adjudicatari haurà de garantir que l'Agència disposi de les capacitats necessàries per fer un ús eficient de la solució proposada. Això implica el lliurament de la següent informació i l'execució de les següents tasques:
    - Documentació/Manuals d'ús del servei.
    - Documentació tècnica de la funcionalitat per a la integració amb l'Índex de Ciberseguretat.
    - Documentació dels procediments de suport.
    - 1 sessió formativa no presencial per a l'ús de la plataforma entre el personal de l'Agència.

2.8.2 Prestació

Es considera la prestació com la fase normal de la prestació del servei. Comença quan la solució proposada és funcional i accessible pels treballadors de l'Agència fins quinze dies abans de que finalitzi la prestació del servei estipulat en el present plec.

A més, durant aquesta fase, estaran vigents els plans de millora continua dels serveis; per aquesta raó els ANS (2.12) s'han de revisar com a mínim cada mes, per tal d'adaptar-los a l'evolució en la prestació dels serveis i a les variacions atenent a les necessitats de l'Agència.

2.8.3 Devolució

Fase que s'emmarca al final de la prestació, un cop s'hagi comunicat la cancel·lació del contracte, i que comença quinze dies abans de l'extinció d'aquest. Durant aquesta fase hi haurà coexistència amb un nou adjudicatari fins que es transfereixin els serveis a aquest.

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

Tot el material i la informació generada, és propietat de l'Agència i romandrà, a l'Agència un cop acabada la prestació del servei.

2.9 Millores

Seran valorades positivament les propostes per part del licitador que suposin una millora o un valor afegit en els següents àmbits.

- La inclusió de mètriques de valor addicionals per a les evidències recollides.
- La inclusió de mètriques útils per al càlcul del *Global Cybersecurity Index* (GCI) de la ITU.
- La inclusió de mecanismes addicionals per a la recollida d'evidències relatives a la fuga o exposició de dades personals, com credencials
- Possibilitat de comparar el nivell de maduresa en ciberseguretat de Catalunya amb un nombre de països per sobre dels 5 mínims establerts.
- Llicències per a la visualització d'entitats per sobre del total de 100 llicències requerides.
- Llicències temporals per a visualització d'entitats per sobre del total de 10 llicències requerides.
- Sessions formatives als treballadors de l'Agència per sobre del mínim d'1 requerida.
- Subministrament de l'històric d'evidències recollides a nivell territorial de Catalunya per a un període majors del mínim d'1 mes requerit (en qualsevol format estàndard i suport).
- Enriquiment de les capacitats del licitador amb capacitats addicionals aportades per mitjà de la col·laboració amb tercers.
- Planificar recursos addicionals per donar resposta puntual a les necessitats de l'Agència, si és requerit.

2.10 Aspectes generals de l'expedient

2.10.1 Establiment del servei dins de l'àrea d'ESG

Inicialment, i en el període de les dues setmanes posteriors a l'adjudicació d'aquest contracte, l'adjudicatari analitzarà la situació actual de l'Agència amb l'objectiu de definir el detall d'un

model de gestió del servei que tingui en compte les millors pràctiques i, com a mínim, els següents punts:

- Procediments.
- Formularis i plantilles de suport.
- Model de *reporting* i seguiment d'indicadors.
- Eines de suport a la gestió.
- I tot allò que pugui ser requerit pel seu correcte funcionament.

Aquest nou model proposat, haurà de ser validat pel responsable de l'àrea d'ESG i estarà subjecte a un procés de revisió i millora contínua per part de l'adjudicatari, durant tota la durada del contracte.

En la fase de licitació, el licitador haurà de presentar en la seva oferta propostes i exemples concrets de procediments, plantilles, lliurables, etc. que donin resposta al conjunt dels punts anteriors. D'igual manera, el licitador d'aquesta oferta haurà de presentar un pla d'actuació detallat que garanteixi les fases d'inici de la prestació del servei o la transició del mateix, la fase de prestació del servei i la fase de devolució d'aquest.

2.10.2 Governança del servei

Per realitzar la governança del servei, l'adjudicatari seguirà la metodologia que s'hagi adoptat en la fase d'establiment del servei per tal que la gestió de les tasques i el seu seguiment siguin àgils, efectius i eficients. El personal de l'adjudicatari reportarà directament al responsable de l'àrea d'ESG o a qui aquest designi, l'estat, l'evolució i els riscos de les tasques del servei.

L'Agència contempla, com a mínim, les fases i tasques en l'àmbit de la gestió del servei que es descriuen a continuació.

2.10.2.1 Planificació

La fase de planificació esdevé la més important i és on cal dedicar més esforços. Amb l'equip del servei definit, el personal de l'adjudicatari liderarà i coordinarà l'equip per afrontar entre d'altres, les tasques de:

- Identificació del personal de l'equip de treball.
- Definició dels rols i les responsabilitats.
- Creació de la llista detallada de tasques.
- Estimació de temps i costos.
- Definició de la planificació de les tasques.
- Anàlisi de riscos i accions de resposta

Aquest equip de treball haurà de coincidir amb l'inclòs en la seva oferta i que ha estat mereixedor de puntuació.

2.10.2.2 Execució

El personal de l'adjudicatari realitzarà un seguiment de l'evolució de les tasques i en la realització entre d'altres, de les tasques següents:

- Seguiment del grau d'assoliment de les tasques i dels processos

- Gestió de canvis de les tasques (requeriments, abast, planificació).
- Gestió dels recursos.
- Definició i extracció d'indicadors de seguiment de l'estat i l'evolució.
- Gestió de les expectatives dels interessats.
- Creació d'una carpeta del servei per emmagatzemar documentació generada.

2.10.2.3 Monitorització i control

Durant tota la durada del servei, el personal de l'adjudicatari adoptarà també la figura de control de cara a poder explicar l'evolució de les tasques a les capes superiors de l'Agència. Entre altres tasques caldrà:

- Analitzar i avaluar la realització de les tasques.
- Aprovar / refusar / comunicar els canvis.
- Actualitzar la planificació de les tasques.
- Informar als interessats.
- Controlar la qualitat de les tasques.
- Gestionar el risc.
- Gestionar les desviacions en pressupost i cronograma.

2.10.3 Innovació

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

El licitador haurà d'incloure a la seva oferta propostes d'innovació que permetin la millora i evolució dels serveis objecte de la present licitació, mitjançant el desplegament de solucions i processos capdavanters. El Pla d'innovació, durant l'execució del servei i a partir del coneixement adquirit, ha de determinar, proposar i implantar processos d'innovació que permetin millorar i/o renovar l'eficiència d'eines i processos, resoldre problemes complexos d'implantació, assolir millores en les metodologies emprades i/o permetre la renovació d'elements ja existents (eines, maquinari, etc.).

2.10.4 Funcions transversals

Tot i que l'activitat principal de l'equip estarà centrada en l'execució de les funcions relacionades amb la prestació d'un servei de suport a la l'àrea d'ESG, s'ha de contemplar la necessitat d'una sèrie de tasques transversals per dotar de coherència i integritat a totes les funcions executades a l'Agència:

- Participar en el model de relació amb els clients i proveïdors de l'Agència, involucrant-se amb ells segons les necessitats de seguretat, els informes de seguiment requerits i les tipologies d'activitat.
- Gestionar les reunions i els conflictes que puguin aparèixer durant l'execució de les tasques.
- Generar actes de les reunions internes i les realitzades amb tercers, identificant clarament els participants les tasques tractades i els acords assolits.

- Mantenir una comunicació fluida amb els diferents lots del present plec i entre els serveis i àrees de l'Agència.
- Alineació i orientació dels projectes per a la consecució dels objectius estratègics de l'Agència.
- Generar els indicadors, informes d'activitat i mètriques de l'activitat del servei.

2.11 Acords de nivell de servei (ANS) i penalitzacions

L'adjudicatari resta obligat al compliment de l'execució total de les prestacions recollides en les ofertes que doni compliment als present plec i a les prescripcions del contracte.

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

El model de penalitzacions que s'aplicaran per l'incompliment dels indicadors i Acords de Nivell de Servei (ANS) definits, d'acord amb els criteris, quantificació i mètode de càlcul són els establerts a la clàusula 26 del Plec de Clàusules Administratives Particulars.

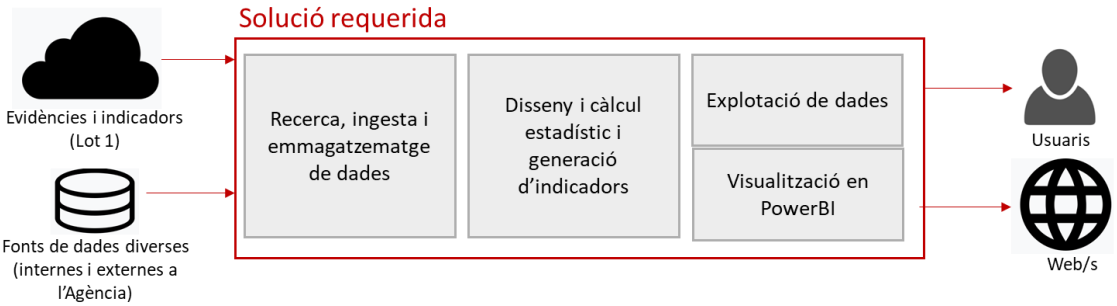
2.1 Indicadors i acords de nivell de servei

Tipus	Nom	Descripció	Formula de càlcul / Eines	Periodicitat	Llindar Inicial (Li)	Llindar Final (Lf)	Penalització Màxima
Personal	Rotació de personal	Índex de rotació del personal presencial en el servei	Índex de rotació de personal = (((A + D)/2) *100)/ES A = Admissions de personal presencial en el servei dins del període considerat. D = Desvinculacions de personal presencial en el servei dins del període considerat. ES = Número d'efectius del servei segons s'estableix en la proposta de servei pel període considerat; si hagués alguna ampliació del servei en número de recursos humans durant el període considerat, es considerarà el valor ponderat al temps d'aplicabilitat.	Mensual	N/A	N/A	% Índex de Rotació x Import de la factura mensual
Personal	Termini per la reposició de recursos	Termini de substitució d'un recurs per un altre, tant sigui per baixa o per rotació de personal	Dies de desviament respecte el termini de reposició de recursos definit	Per recurs	5 dies	15 dies	Import equivalent a les hores de no disponibilitat del recurs.
Disponibilitat	Nivells de suport en la resposta i resolució d'incidències que afectin a la disponibilitat o qualitat del servei	Retard excessiu en la resposta i resolució d'incidències que afectin a la disponibilitat o qualitat del servei	Hores des de l'avís de la incidència fins que se soluciona	Per incidència	4h	8h	Import de 2h de servei per cada hora de no disponibilitat o qualitat degradada del servei
Gestió	Nivells de suport en la resposta a consultes, peticions de suport analític o en l'ús de la solució del servei	Retard excessiu en la resposta a peticions de suport	Hores des de la petició fins que es rep una resposta	Per petició	2 dies naturals	5 dies naturals	1% del cost mensual del servei per dia de retard en la resposta
Qualitat	Volum mig d'evidències diàries en un període d'un mes per sota del valor ofertat	Desviament en el nombre d'evidències recollides que pot afectar en la fidelitat dels indicadors	Nombre mig d'evidències per dia en un període mensual	Mensual	0%	10%	5% del cost mensual del servei
Qualitat	Qualitat dels lliurables del servei (indicadors)	Grau de satisfacció del client respecte dels informes	Puntuació de 1 a 10 segons enquestes de satisfacció al client	Mensual	8	5,5	20% del cost mensual del servei
Terminis	Desviació sobre el termini de lliurament pactat de l'informe anual	Retard en dies en el lliurament de l'informe	Dies de desviació	Per Projecte	5 dies	10 dies	2% del cost mensual del servei per dia de retard en el lliurament

3 LOT 2: DISSENY, DESENVOLUPAMENT, IMPLANTACIÓ, POSADA EN SERVEI I MANTENIMENT DE L'ÍNDEX DE CIBERSEGURETAT DE CATALUNYA

3.1 Objecte

La supervisió d'un conjunt adequat d'indicadors que, en matèria de ciberseguretat, descriguin l'activitat a la xarxa en el territori de Catalunya, és cabdal per obtenir capacitats per al control i la investigació dels riscos, planificar programes de mitigació i fomentar una acció ràpida i efectiva amb l'objectiu de millorar la seguretat i la confiança digitals. En aquest sentit, es requereix la contractació d'un servei que dissenyi, desenvolupi, implanti, posi en servei i mantingui un sistema d'informació on s'aglutinin, es processi i s'emmagatzemi estructuradament la informació provinent de diferents fonts amb l'objectiu de visualitzar un conjunt d'indicadors que descriguin, de forma entenedora, les característiques i evolució de la ciberseguretat a Catalunya. La solució desenvolupada ha de recollir les evidències, mètriques i indicadors de la solució per a la monitorització de la ciberseguretat a Catalunya (Lot 1).



Esquema conceptual de la integració del servei del Lot 2

L'adjudicatari dissenyarà i es responsabilitzarà del desplegament de l'activitat relacionada amb l'Índex de ciberseguretat orientada a recopilar i albergar les dades analítiques necessàries per monitorar, de forma contínua i objectiva, la maduresa en ciberseguretat i el nivell de confiança digital a Catalunya per àmbit sectorial i en un context global. Haurà de desenvolupar les activitats necessàries per a l'obtenció d'un centre d'observació operatiu que esdevingui referencial en l'àmbit de la ciberseguretat catalana.

L'Índex de ciberseguretat implica identificar la informació a recollir, habilitar els sistemes per a la seva recollida, emmagatzematge, explotació i compartició. És una iniciativa en resposta a un objectiu estratègic de llarg recorregut, atès que tindrà per endavant la tasca de detectar la informació necessària per a l'ampliació i millora continuada dels seus resultats.

3.2 Objectius del Servei

Els objectius de la present licitació són:

- Desenvolupar i mantenir un Índex de ciberseguretat i fer difusió d'indicadors representatius del nivell de maduresa en ciberseguretat i de la confiança digital a Catalunya.
- Definir i mantenir una estructura d'indicadors de ciberseguretat propis amb una base històrica consultable que permeti visualitzar-ne l'evolució i tendències.
- Integrar la informació i indicadors generats pel servei al sistema de *business intelligence* (PowerBI) emprat com a repositori d'indicadors compartits de l'Agència.
- Participar en la definició i consens amb entitats col·laboradores de l'Agència del model de recollida, anàlisi i comunicació de dades, mètriques i indicadors.
- Definir i consensuar els indicadors necessaris per poder avaluar l'estat de la ciberseguretat a Catalunya i integrar-los en el servei de l'Índex de Ciberseguretat de Catalunya.
- Identificar les mètriques i indicadors necessaris per avaluar l'impacte d'accions (plans de comunicació i conscienciació) sobre el nivell de maduresa en matèria de ciberseguretat i la confiança digital de la societat catalana
- Obtenir indicadors útils per identificar activitats, capacitats, necessitats i oportunitats per al sector de la ciberseguretat a Catalunya.
- Obtenir indicadors útils per identificar l'evolució del teixit empresarial de l'ecosistema de la ciberseguretat (p. ex. nombre d'empreses, volum de negoci, etc.) i els seus professionals (p. ex. estudis, estudiants titulats, nombre de professionals, certificats, remuneració econòmica, etc.).
- Obtenir indicadors útils per representar i divulgar, tant a nivell nacional com internacional, les principals iniciatives i assoliments de la ciberseguretat a Catalunya.
- Obtenir indicadors útils per identificar i definir les principals amenaces de ciberseguretat que poden tenir impacte en la ciutadania i el teixit productiu a Catalunya.
- Obtenir indicadors útils per facilitar el càlcul del Global Cybersecurity Index (GCI) de la ITU de forma continuada en el temps.
- Identificar fonts d'interès que puguin i/o hagin d'aportar les mètriques definides (CSIRT sectorials, APC (Administració Pública Catalana), IdesCAT, Agència Catalana de Consum, Institut d'Estudis de la Seguretat, Universitats i Centres de Recerca, empreses privades i d'altres que puguin resultar rellevants).
- Establir canals de comunicació de les troballes de l'Índex de ciberseguretat i fer-ne un seguiment mitjançant indicadors clau per fomentar una acció ràpida i efectiva.
- Promoure l'explotació i comunicació d'indicadors, així com la compartició d'informació de mètriques representatives en general, entre els actors implicats, tant per l'àmbit públic com pel privat.
- Arran de la informació de l'Índex de Ciberseguretat, col·laborar amb el Servei d'ATS de l'Agència per facilitar l'elaboració d'un estudi estadístic i comparatiu sobre el nivell de ciberseguretat del sector privat català i un mapa dels riscos de ciberseguretat a Catalunya.

— Disposar de capacitats i eines necessàries per establir una col·laboració eficaç i eficient pel que fa a la recollida de mètriques i indicadors i la provisió d'aquests en resposta a peticions o per donar suport a emergències.

3.3 Activitats del Servei

El servei consisteix en el disseny, desenvolupament, implantació, posada en servei i manteniment d'un Índex de Ciberseguretat capaç de recollir les dades i explotar-les analíticament amb la finalitat d'avaluar de forma objectiva el nivell de maduresa en matèria de ciberseguretat i confiança digital a Catalunya. Per a la realització aquest servei, l'adjudicatari serà responsable de dur a terme les activitats descrites a continuació, a més d'allò que expliciti en la seva oferta.

3.3.2 Disseny i implementació de la plataforma tecnològica al núvol

L'adjudicatari, d'acord amb la planificació pel desenvolupament del projecte detallada en la seva oferta, serà responsable de dissenyar els requeriments específics de la infraestructura tecnològica del núvol que serà on s'allotjarà l'Índex de Ciberseguretat.

Es dissenyaran els mòduls d'ingesta i processament de dades des de fonts diverses, el mòdul d'emmagatzematge i el mòdul de visualització segons s'estableix en el plec (3.4). Durant la fase del disseny del sistema d'informació, caldrà definir el motor de la base de dades estructurada i la seva organització operacional, modularitat i les relacions entre els diferents elements. Així mateix, caldrà tenir en compte que aquesta base de dades serà la base de possibles evolucions i ampliacions, de manera que haurà d'estar degudament preparada. Addicionalment, s'implementaran els canals necessaris per a la integració amb altres sistemes existents a l'Agència, com l'Eina d'emmagatzematge i anàlisi de notícies de ciberseguretat del Servei d'ATS, la base de dades corporativa de *business intelligence* (actualment PowerBI) i la informació originada en el SOC (*Security Operations Center*) de l'Agència.

S'utilitzarà l'entorn d'Azure sota les condicions del contracte marc entre Microsoft i el Centre de Telecomunicacions i Tecnologies de la Informació (CTTI).

L'entorn haurà de ser dissenyat i configurat de manera segura, de forma alineada amb les recomanacions i polítiques de l'Agència, i serà degudament testejat per l'adjudicatari per experts en ciberseguretat. Certificarà amb un informe l'anàlisi de ciberseguretat realitzat i les mesures aplicades a l'Agència.

3.3.3 Ingesta, processament i emmagatzematge diari de les dades originades pel Servei per a la monitorització de la ciberseguretat a Catalunya (Lot 1)

Una vegada es disposi de la plataforma de l'Índex de Ciberseguretat al núvol, l'adjudicatari haurà d'implementar la comunicació amb el sistema d'informació del Servei per a la monitorització de la ciberseguretat a Catalunya (Lot 1) per mitjà de l'API que li subministri l'adjudicatari d'aquest altre servei.

De forma prioritària per sobre qualsevol altra font, l'adjudicatari procedirà a la ingesta, processament i emmagatzematge de la informació que, amb una periodicitat diària i de forma automatitzada, l'adjudicatari del Lot 1 proveeixi via API. Aquesta informació serà una combinació d'evidències de xarxa recollides al territori de Catalunya i indicadors (visió orientativa a l'annex I).

Sempre que sigui possible, les dades que entrin a formar part de l'Índex disposaran clarament definits els següents atributs:

- Marc temporal: en general, serà l'any natural o altres períodes menors (dia, mes, trimestre, semestre, etc.).
- Marc territorial: seran coordenades, atributs georrefernciable (p. ex. les IP) o demarcacions territorials (p. ex. nucli de població, municipis, comarques, províncies, etc.).

En l'abast del desenvolupament actual, no es preveu la càrrega en *stream* des de fonts *big data*.

3.3.4 Recerca i càrrega de noves fonts d'informació

L'adjudicatari serà responsable de tot el procés relatiu a la recerca, identificació i ingesta de dades des de noves fonts d'informació. De manera proactiva i continuada realitzarà les tasques següents::

- Identificació: anàlisi de necessitats o oportunitats de l'Agència, fonts d'informació externes i internes per donar-hi resposta.
- Planificació: recerca de novetats i seguiment sistemàtic de noves dades i indicadors.
- Cerca i tractament: recollida, validació, preparació, tractament inicial, anàlisi matemàtic-estadístic.

L'adjudicatari haurà de donar solucions a la càrrega de dades massiva, eficient i eficaç al sistema des de fonts heterogènies, estructurades i no estructurades, subministrades des de diferents canals (correu electrònic, API, servei web, suport físic, etc.), amb fluxos variables i diferents formats. La càrrega de dades ha de poder fer-se, sempre que sigui possible, mitjançant mecanismes automatitzats de sincronització periòdica o, en el seu defecte, de forma manual.

S'hauran de complimentar degudament les metadades per a tota la informació carregada al sistema d'acord amb estàndards i millors pràctiques, la qual haurà de ser consultable pels usuaris consumidors de l'Índex de Ciberseguretat.

Serà especialment rellevant el subministrament d'una solució per a l'anàlisi i càrrega d'enquestes, d'abast nacional, estatal o internacional, i l'objectiu serà poder disposar d'escenaris confluents per a la comparació de resultats amb relació a la realitat de Catalunya, sempre i quan aquesta informació estigui disponible.

També s'hauran de recollir les dades necessàries i generar els indicadors adients per facilitar el càlcul del GCI (Global Cybersecurity Index) de la ITU.

3.3.5 Analítica i explotació de dades

L'adjudicatari serà responsable de l'explotació de les dades recollides per tal de dissenyar indicadors representatius que aportin una visió objectiva i seguida en el temps, així com serà responsable del seu anàlisi amb l'objectiu d'avaluar, de forma objectiva, entre d'altres:

- L'evolució de l'estat del nivell de maduresa de la ciberseguretat a Catalunya.
- El nivell de confiança digital de la societat catalana i l'impacte dels plans de comunicació i conscienciació sobre aquesta.
- Principals ciberamenaces en diferents àmbits, com sectors econòmics, departaments de la Generalitat de Catalunya, la ciutadania (en especial els col·lectius en risc, com la gent gran i els menors) i el teixit empresarial.
- L'evolució de la implantació d'esquemes de certificació en matèria de ciberseguretat.

- La comparació de Catalunya respecte mètriques i indicadors externs generats en estudis de referència d'àmbit nacional o internacional.

En aquest sentit, els indicador poden ser de diferent tipologia:

- Identificació dels principals resultats o rankinqs.
- Comparativa d'un indicador específic a nivell de sector.
- Comparativa i contextualització d'un cert indicador de Catalunya dins d'un espai internacional.
- Identificació de l'evolució d'un indicador específic durant el temps.
- Identificació de la concentració d'un cert paràmetre a nivell geogràfic.
- Promig d'un indicador respecte el nombre d'habitants o nombre de dispositius connectats (IP) de Catalunya.

3.3.6 Visualització gràfica

A partir de les dades incorporades l'Índex de Ciberseguretat, es dissenyaran indicadors que tinguin la capacitat de fer visible la situació de la ciberseguretat a Catalunya mitjançant la generació de taules i gràfics dinàmics (barres, formatges, lineals, etc.). L'adjudicatari serà responsable del disseny, càlcul i implementació gràfica dels indicadors.

L'Agència disposa de PowerBI per a la implementació gràfica dels indicadors i aquesta serà la solució emprada. Els indicadors podran ser de dos tipus, restringits o públics. Els restringits seran accessibles pels treballadors de l'Agència a través dels quadres de comandament elaborats en PowerBI al Tenant Corporatiu. Els indicadors públics estaran pensats i dissenyats per a una difusió oberta des del lloc web que es determini en un futur on allotjar l'Índex de Ciberseguretat. En qualsevol cas, l'adjudicatari haurà de preparar l'entorn PowerBI degudament per tal que esdevingui el concentrador de la informació consultable tant pels treballadors de l'Agència com per la pàgina web on es publiquin.

Els quadres de comandament han de representar els indicadors per tal de donar sentit a grans volums de dades complexes, difícils d'entendre d'altra manera. Han de resumir la informació centrant-se en allò important sense perdre els detalls, facilitant la detecció de tendències, anomalies, agrupacions, relacions, etc.

La navegació per les dades haurà d'incorporar un arbre de continguts per explorar les dades organitzades en un nombre arbitrari de nivells de jerarquia.

La visualització gràfica dels indicadors haurà de possibilitar, com a mínim i sempre que sigui possible, els següents filtres:

- Tipologia d'indicador.
- Sector econòmic.
- Període temporal.
- Àmbit geogràfic (s'inclourà un visor geogràfic on ubicar tota la informació georreferenciable com les adreces IP).

A més del filtratges i segmentació, sempre que sigui possible, s'incorporaran les següents capacitat a les visualitzacions:

- Capacitat de navegació (anar del general al detall, p. ex. en gràfics jeràrquics).
- Ordre de les dades (alfabètic, quantitatiu, etc.).
- Interactivitat (p. ex. simulant l'evolució de les dades en el temps).

- Mostra d'atributs extra (p. ex. anotacions explicatives, dates rellevants, etc.).
- Relació de dues visualitzacions i, d'aquesta manera, generant interactivitat mútua.

3.3.7 Posta en valor i explotació

L'adjudicatari serà responsable de la posta en valor dels elements gràfics generats amb la seva descripció i el seu significat amb l'objectiu d'interpretar la situació de la ciberseguretat a Catalunya que permeti donar suport a la presa de decisions a tots els nivells.

L'adjudicatari serà proactiu en definir tècniques i estratègies d'explotació dels productes gràfics generats amb l'objectiu de maximitzar la seva distribució i impacte fent ús dels instruments existents a l'Agència per a la difusió de la informació: correu electrònic, pàgina web, xarxes socials, etc.

Entre d'altres possibilitats, a partir de les dades i els indicadors de l'Índex, l'adjudicatari haurà de complir les següents necessitats:

- A partir dels indicadors, l'adjudicatari tindrà encàrrecs per elaborar quadres de comandament especialment dissenyats i dirigits a potencials destinataris específics com, per exemple, als diferents Departaments de la Generalitat de Catalunya o altres entitats col·laboradores.
- Durant la primera meitat de l'any, el servei d'ATS elaborarà un estudi estadístic i comparatiu sobre el nivell de ciberseguretat del sector privat català, amb la definició de les principals amenaces que poden tenir impacte en el teixit productiu, conjuntament amb l'elaboració i publicació de mapes de riscos de ciberseguretat a Catalunya. L'adjudicatari generarà els indicadors necessaris per ser utilitzats com a element central del document on es desenvoluparà el seu anàlisi i interpretació, i s'inclouran mesures per a la millora de la ciberseguretat, ja sigui en concepte de regulació, dinamització o propostes innovadores per incentivar l'intercanvi de productes i serveis.
- L'Agència podrà dirigir requeriments específics a l'adjudicatari per a l'elaboració d'informes o generació d'indicadors que puguin ser necessaris per a donar resposta a necessitats puntual.

3.3.8 Manteniment i evolució de l'Índex

L'adjudicatari serà responsable del manteniment de l'Índex, garantir el seu funcionament i la seva usabilitat:

- Manteniment reactiu i incidències
  - L'adjudicatari haurà d'utilitzar una adreça de correu electrònic corporatiu de l'Agència per a la recollida d'incidències i procedirà a emprendre les accions de manteniment correctiu d'acord amb les prioritats acordades amb l'Agència.
  - El temps de resposta (SLA) per incidències identificades ha de ser d'un màxim de 4 hores dins del servei 8x5 establert, coincidint amb l'horari d'oficina de l'Agència.
- Manteniment proactiu i evolutiu
  - L'adjudicatari serà proactiu amb relació a la proposició de nous evolutius que mantinguin el sistema d'informació de l'Índex actualitzat.
  - L'adjudicatari haurà de descriure en detall la metodologia de gestió dels manteniments proactius i dels nous desenvolupaments que s'acordin.

- En els casos de manteniment evolutiu, l'adjudicatari planificarà el cost previst en hores de treball i data de lliurament abans d'iniciar la feina.

3.3.9 Formació i documentació

L'adjudicatari s'ocuparà d'elaborar lliurables per a la documentació i comunicació de l'evolució del projecte i subministrarà els següents serveis:

- Base de dades documental, fitxes o equivalent amb la descripció, càlcul i interpretació dels diferents indicadors generats.
- Document amb les especificacions tecnològiques i configuració de l'Índex de Ciberseguretat actualitzat amb una periodicitat mínima mensual.
- Manual d'ús i administració de l'Índex de Ciberseguretat actualitzat amb una periodicitat mínima mensual.
- Mapa de processos que permetin visualitzar els principals elements de l'Índex de Ciberseguretat i la descripció de les interrelacions amb les diferents fonts d'informació i consumidors actualitzat amb una periodicitat mínima mensual.
- Butlletins mensuals enviats a tots el personal de l'Agència amb informació sobre els nous indicadors o quadres de comandament produïts per promoure el seu coneixement i ús.

Quan l'Índex de ciberseguretat estigui en producció, l'adjudicatari realitzarà formació al personal de l'Agència per al seu coneixement, ús i aprofitament. Així mateix, l'Agència podrà sol·licitar posteriors sessions per informar dels evolutius realitzats.

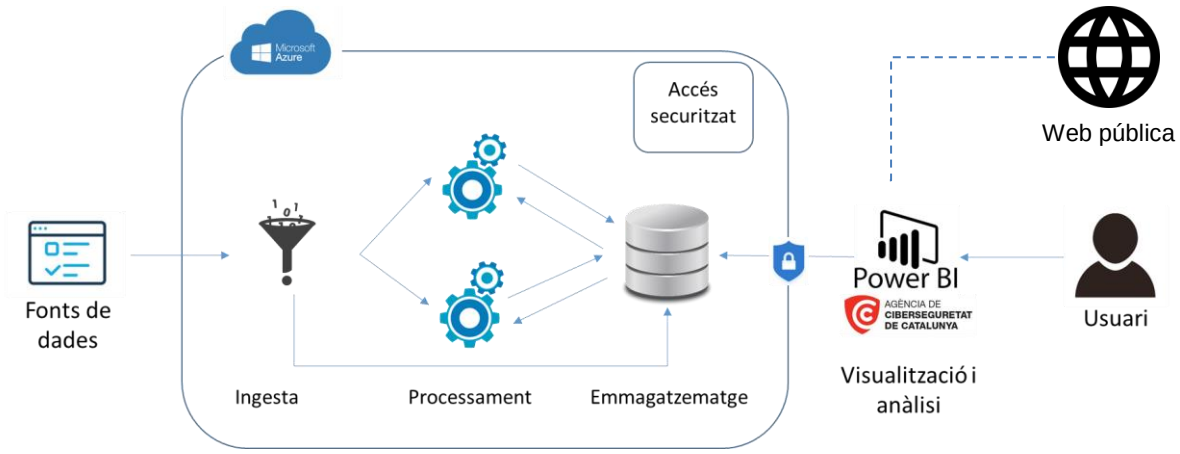
3.4 Requeriments tecnològics de l'Índex de Ciberseguretat

La implementació pot basar-se en l'adopció d'una solució integral o en la combinació d'un conjunt d'eines individuals, sempre que siguin compatibles i integrables amb mòduls estàndard, aprofitant els avantatges i beneficis de triar les millors eines especialitzades per a cada component de l'arquitectura.

En tots els casos, els productes triats hauran de disposar d'un ampli reconeixement i estandardització en el mercat i comptar amb implantacions en el sector públic.

Els sistemes, eines i plataformes i tota la infraestructura s'han de proporcionar com a servei. El licitador haurà de proposar l'arquitectura necessària tenint en compte que aquesta s'allotjarà en el núvol Azure, adaptant-se a les característiques mínimes recollides en aquest plec.

A continuació, es presenta una proposta genèrica d'arquitectura per a dur a terme el servei:



Model esquemàtic d'arquitectura per l'Índex de Ciberseguretat

3.4.2 Mòduls d'ingesta i processament de dades

S'haurà de proporcionar una plataforma de processament i logística de dades que permeti, a través d'eines ETL (*Extract, Transform, Load*), l'extracció de diferents fonts, transformació i processament de les dades, i càrrega a la base de dades de l'Índex de Ciberseguretat.

El mòdul d'ingesta proposat haurà de complir, com a mínim, amb les següents característiques:

- Ingesta d'informació sense afectació al rendiment dels serveis de les fonts d'origen i de destí.
- Diferents connectors d'origen per a BBDD, xarxes socials, cues, etc.
- Connexió a diferents sistemes d'emmagatzematge.
- Transformació entre diferents formats de dades com, per exemple, JSON, XLSX, TXT, XML, Avro o CSV.
- Múltiples instàncies.
- Admissió de fonts disperses de diferents formats, esquemes, protocols, velocitats i grandàries, ubicacions geogràfiques, màquines, etc.
- Rastreig de dades en temps real.

3.4.3 Mòdul d'emmagatzematge

S'haurà d'aprovisionar d'una base de dades relacional per a l'emmagatzematge de la informació. La base de dades proposada haurà de donar resposta a les següents característiques estàndard:

- Funcionament basat en client i servidor.
- Compatibilitat amb SQL.
- Configuració de vistes.
- Que permeti procediments emmagatzemats per a incrementar l'eficàcia de les implementacions.
- Automatització de tasques, desencadenants.

- Gestió de transaccions que permeti avalar que tots els procediments s'estableixen correctament.
- Escalable.
- Protegida contra accessos no autoritzats.
- Compatible amb tecnologies BI.

No es preveuen necessitats d'emmagatzematge *big data* o càrrega de dades no estructurades.

3.4.4 Mòdul de visualització

Actualment, l'Agència disposa de l'eina PowerBI. El servei s'integrarà amb aquesta per al desenvolupament dels informes i visualització dels indicadors.

- Es crearan quadres de comandaments diferents per a cadascuna de les fonts, així com indicadors generals que es definiran durant el desenvolupament de l'Índex de Ciberseguretat.
- L'accés quedarà restringit segons el perfil dels diferents usuaris.
- Ha de permetre la publicació en diferents formats: obert (per exemple, a la web o webs de determini l'Agència), restringit, intern, etc.

3.4.5 Entorns de treball

L'adjudicatari prestarà els serveis en els següents entorns de treball:

- Entorn de Desenvolupament i validació: on es permeti realitzar els desenvolupaments i accions necessàries sobre la base instal·lada, així com les correccions funcionals i tècniques.
- Entorn de Producció: on accediran els usuaris de l'Agència per a utilitzar i explotar la informació.

Totes les eines, productes, plataformes i infraestructures dels entorns de desenvolupament que formin part d'aquesta arquitectura, hauran de ser dissenyats i requerits per l'adjudicatari, i subministrats per l'Agència.

3.5 Mitjans humans i tècnics

3.5.1 Especificacions mínimes de l'equip i requisits professionals

Per tal de donar resposta a les activitats i productes descrits, l'àrea d'ESG requereix la incorporació dels recursos i perfils que s'assenyalen al quadre resum de característiques del PCAP i que constitueixen la solvència mínima requerida.

Advertència Important: s'està demanant una oferta estructural de coneixement, en cap cas una oferta d'hores de perfils. Recordem que la inclusió de dades que s'hagin de valorar en el sobre C a l'oferta tècnica (sobre B) implica l'exclusió automàtica del licitador.

3.5.1.1 Dedicació

La dedicació mínima dels perfils estipulats, podent concentrar-se de forma desigual en les diferents fases del projecte, és la següent:

Consultor especialista en anàlisi de dades	**0,25 FTE**
Especialista estadístic	**0,5 FTE**
Ingestador de dades	**0,5 FTE**
Especialista en PowerBI	**0,5 FTE**
Especialista en infraestructures *cloud*	**0,10 FTE**
TOTAL	**1,85 FTE**

3.6 Fases de la prestació del Servei

Els licitadors hauran de presentar dins la seva oferta tècnica el pla d'actuació detallat per tal d'aconseguir una transició adequada que asseguri la transferència de coneixement més adequada per a l'inici de la prestació del servei i en la posterior devolució a la seva finalització.

3.6.2 Transició i inici

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

Amb l'objectiu d'aconseguir un inici eficient, cal assegurar que es duran a terme les següents activitats:

- Adquisició del coneixement de l'estat actual de les tasques dels serveis. L'adjudicatari haurà de parlar amb els responsables de l'Agència per tal d'entendre el funcionament i la situació de l'actual servei.
- Adquisició del coneixement de com operar les eines actuals disponibles. L'adjudicatari haurà de recollir les especificacions tècniques i resoldre dubtes.
- Adquisició del coneixement del funcionament del servei, les particularitats i de les millors pràctiques.

3.6.3 Prestació

Es considera la prestació com la fase normal de la prestació del servei. Comença quan els processos d'implantació del nou model d'oficina hagin acabat fins quinze dies abans de que finalitzi la prestació del servei estipulat en el present plec.

A més, durant aquesta fase, estaran vigents els plans de millora continua dels serveis; per aquesta raó els ANS (3.2) s'han de revisar com a mínim cada mes, per tal d'adaptar-los a l'evolució en la prestació dels serveis i a les variacions atenent a les necessitats de l'Agència.

3.6.4 Devolució

Fase que s'emmarca al final de la prestació, un cop s'hagi comunicat la cancel·lació del contracte, i que comença quinze dies abans de l'extinció d'aquest. Durant aquesta fase hi haurà coexistència amb un nou adjudicatari fins que es transfereixin els serveis a aquest.

L'adjudicatari haurà de procurar la metodologia, eines i recursos necessaris per tal de traspassar adequadament el servei a altres possibles futurs adjudicataris. En especial, es requereix la descripció detallada de la metodologia relativa als sistemes en els quals s'ha treballat durant l'execució del contracte.

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

Els mitjans tècnics que el proveïdor sortint hagi proporcionat per tal de desenvolupar la seva tasca (3.1.5) hauran de ser degudament esborrats i tota la informació traspassada a qui l'Agència designi. La devolució de les eines es regirà segons l'estipulat en aquest plec i en les condicions acordades amb l'adjudicatari.

3.7 Indicadors del Servei

El servei fa ús d'un quadre d'indicadors de referència que són indicadors generals de l'entitat i també indicadors de gestió i seguiment de l'evolució de cada activitat.

CAMP	***DESCRIPCIÓ***
Fonts d'informació	Núm. de fonts d'informació integrades a l'Índex de Ciberseguretat
Indicadors	Núm. d'indicadors generats a l'Índex de Ciberseguretat
Ús intern	Estadístiques d'ús (p. ex. usuaris diaris, informació més consultada...) pels usuaris de l'Índex de Ciberseguretat de l'Agència
Ús extern	Estadístiques d'ús (p. ex. usuaris diaris, informació més consultada...) pels usuaris de l'Índex de Ciberseguretat externs a l'Agència
Impacte	Núm. de publicacions de l'Índex de Ciberseguretat en XXSS o mitjans d'informació
Altres	Altres indicadors que es considerin oportuns

Si s'escau, en concordança amb la resta de serveis de l'Agència, els indicadors de mesura i seguiment seran integrats en els Repositoris d'indicadors i d'informació corporatius, per posteriorment ser visualitzats en eines que faciliten la gestió dels mateixos, com ara eines de BI. Aquest procés de càrrega d'informació i visualització dels indicadors és funció del servei de Govern de la Dada de l'Agència, amb el que l'adjudicatari s'ha de coordinar contínuament per garantir una correcta càrrega dels indicadors establerts, i l'evolució dels mateixos. Ara bé, és responsabilitat del servei garantir la qualitat de la informació que genera, establint mecanismes per detectar errades i fer les actuacions corresponents per la seva correcció.

3.8 Millores

Seran valorades positivament les propostes per part del licitador que suposin una millora o un valor afegit en els següents àmbits.

— Proposta d'alternatives que permetin una major eficiència amb els recursos disponibles mitjançant eines informàtiques que permetin automatitzar els procediments com, per exemple, mitjançant solucions RPA (*Robotic Process Automation*) o *Machine Learning*.

- Enriquiment del servei presencial proposat amb l'oferta de capacitats addicionals aportades per la pròpia empresa o amb la col·laboració de tercers i més enllà dels recursos requerits.
- Possibilitats de fer ús de fonts d'informació professionals del licitador o de tercers que permetin enriquir el servei.
- Integració d'elements addicionals o implementació de noves funcionalitats que signifiquin una millora substancial de l'Índex de Ciberseguretat.
- Qualsevol aportació a la confecció dels productes destinats a l'explotació de les dades de l'Índex que suposi una millora en quant a estructura o contingut.

Advertència Important: s'està demanant una oferta estructural de coneixement, en cap cas una oferta d'hores de perfils. Recordem que la inclusió de dades que s'hagin de valorar en el sobre C a l'oferta tècnica (sobre B) implica l'exclusió automàtica del licitador.

3.9 Aspectes generals de l'expedient

3.9.1 Establiment del servei dins de l'àrea d'ESG

Inicialment, i en el període de les dues setmanes posteriors a l'adjudicació d'aquest contracte, l'adjudicatari analitzarà la situació actual de l'Agència amb l'objectiu de definir el detall d'un nou model de gestió del servei que tingui en compte les millors pràctiques i, com a mínim, els següents punts:

- Procediments.
- Formularis i plantilles de suport.
- Model de *reporting* i seguiment d'indicadors.
- Eines de suport a la gestió.
- Metodologia.
- I tot allò que pugui ser requerit pel seu correcte funcionament.

Aquest nou model proposat, haurà de ser validat pel responsable de l'àrea d'ESG i estarà subjecte a un procés de revisió i millora contínua per part de l'adjudicatari, durant tota la durada del contracte.

En la fase de licitació, el licitador haurà de presentar en la seva oferta propostes i exemples concrets de procediments, plantilles, lliurables, etc. que donin resposta al conjunt dels punts anteriors. D'igual manera, el licitador d'aquesta oferta haurà de presentar un pla d'actuació detallat que garanteixi les fases d'inici de la prestació del servei o la transició del mateix, la fase de prestació del servei i la fase de devolució d'aquest.

3.9.2 Governança del servei

Per realitzar la governança dels diferents lots, els adjudicataris seguiran la metodologia que s'hagi adoptat en la fase d'establiment del servei per tal que la gestió de les tasques i el seu seguiment siguin àgils, efectius i eficients. El personal de l'adjudicatari reportarà directament al responsable de l'àrea d'ESG o a qui aquest designi, l'estat, l'evolució i els riscos de les tasques del servei.

L'Agència contempla com a mínim, les fases i tasques en l'àmbit de la gestió del servei que es descriuen a continuació.

3.9.2.1 Planificació

La fase de planificació esdevé la més important i és on cal dedicar més esforços. Amb l'equip del servei definit, el personal de l'adjudicatari liderarà i coordinarà l'equip per afrontar entre d'altres, les tasques de:

- Definició dels requeriments detallats, identificats pel personal especialitzat de l'equip de treball.
- Definició del material necessari que cal reservar o adquirir.
- Creació de la llista detallada de tasques.
- Estimació de temps i costos.
- Definició de la planificació de les tasques.
- Definició dels rols i les responsabilitats.
- Anàlisi de riscos i accions de resposta

3.9.2.2 Execució

El personal de l'adjudicatari realitzarà un seguiment de l'evolució de les tasques i en la realització, entre d'altres, de les tasques següents:

- Seguiment del grau d'assoliment de les tasques i dels processos
- Gestió de canvis de les tasques (requeriments, abast, planificació).
- Gestió dels recursos.
- Definició i extracció d'indicadors de seguiment de l'estat i l'evolució.
- Gestió de les expectatives dels interessats.
- Creació d'una carpeta del servei per emmagatzemar documentació generada.

3.9.2.3 Monitorització i control

Durant tota la durada del servei, el personal de l'adjudicatari adoptarà també la figura de control de cara a poder explicar l'evolució de les tasques a les capes superiors de l'Agència. Entre altres tasques caldrà:

- Analitzar i avaluar la realització de les tasques.
- Aprovar / refusar / comunicar els canvis.
- Actualitzar la planificació de les tasques.
- Informar als interessats.
- Controlar la qualitat de les tasques.
- Gestió del risc.
- Gestionar les desviacions en pressupost i cronograma.

3.9.3 Repositoris d'indicadors i informació

L'Agència ha realitzat grans esforços en la conceptualització i estructuració, de tota la informació que els diferents serveis englobats en les diferents àrees generen com a conseqüència de l'execució dels mateixos.

Tota aquesta informació està estructurada i integrada dintre d'un repositori que s'anomena RISC (Repositori d'Informació de Serveis de l'Agència). Aquesta informació de RISC és tractada i analitzada mitjançant una eina corporativa de BI mitjançant la qual els serveis poden analitzar la informació des de diferents perspectives:

- Indicadors de risc (responsabilitat exclusiva del servei de Govern del risc de l'Agència).
- Indicadors operatius dels serveis de l'Agència, on cada servei volca aquella informació que li serveix per fer el seguiment del servei i disposar d'indicadors rellevants del mateix.
- Indicadors per la Direcció de l'Agència.

3.9.3.1 Cicle de vida del Govern de la Dada

Cada servei de l'Agència, com el que és objecte d'aquesta licitació, és responsable de la generació de la informació i indicadors que li són necessaris pel desplegament i execució del seu servei. Cada servei també és encarregat de definir quina informació i quins indicadors s'han de carregar a RISC.

El servei de Govern de la Dada és l'encarregat de la realització dels processos de càrrega (ETL), així com del manteniment i evolució del model de dades de RISC. El servei de Govern de la Dada és el responsable de construir les vistes o QCI en l'eina de BI corporativa, en coordinació amb els diferents serveis i els seus responsables de l'Agència. En aquest sentit, la comunicació amb el servei de Govern de la Dada esdevé un aspecte fonamental per assegurar l'alineament i coordinació en tot moment (assegurament de la qualitat de les dades, indicadors de valor pel servei i l'Agència, entre altres).

La informació dels serveis i els indicadors associats és consultable a través de l'eina de BI. Aquests indicadors són generats i governats per cada servei. Aquests indicadors tenen diferent naturalesa i responen a diferents necessitats del servei, tant operacionals, com de seguiment, volumètrics d'activitat, com de seguretat o de risc particular (vertical), entre d'altres.

3.9.3.2 Govern del Risc de Ciberseguretat de l'Agència

El servei de Govern del Risc de Ciberseguretat de l'Agència, és el servei encarregat de la identificació, gestió i comunicació dels riscs globals que puguin afectar a l'Agència, al model de ciberseguretat que aquest gestiona o al nivell de ciberseguretat de la Generalitat de Catalunya i als seus departaments.

Tots els serveis de l'Agència estan orientats a risc i, per tant, desenvolupen i comuniquen els seus resultats amb una visió "vertical" enfocada a la naturalesa del seu servei. El servei de Govern del Risc té una visió transversal i estudia els riscos amb aquest impacte horitzontal a l'organització.

El servei de Govern del Risc és el principal consumidor d'informació del repositori d'informació de l'Agència (RISC) donat que aquest repositori li aporta la informació i indicadors precisos per avaluar el nivell de risc a la Generalitat (dels actius TIC, del departament, dels proveïdors). El Govern del risc utilitza la plataforma BI corporativa i el repositori d'informació corporatiu (entre altra informació que pugui recollir no estructurada) per fer el seguiment i *reporting* dels riscos de seguretat a la Generalitat de Catalunya.

Per tant, la coordinació dels serveis adjudicats amb el servei de govern del risc és un aspecte fonamental per assegurar que informació de qualitat és bolcada en primera instància al repositori RISC i posteriorment és explotada i analitzada mitjançant les eines de BI que l'Agència posa a disposició del servei.

3.9.4 Innovació

En un món tant canviant com és el de la ciberseguretat, és 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.

El licitador haurà d'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. El Pla d'innovació, durant l'execució del servei i a partir del coneixement adquirit, ha de determinar, proposar i implantar processos d'innovació que permetin millorar i/o renovar l'eficiència d'eines i processos, resoldre problemes complexos d'implantació, assolir millores en les metodologies emprades i/o permetre la renovació d'elements ja existents (eines, maquinari, etc.).

3.9.5 Funcions transversals

Tot i que l'activitat principal de l'equip estarà centrada en l'execució de les funcions relacionades amb la prestació d'un servei de suport a la l'àrea d'ESG, s'ha de contemplar la necessitat d'una sèrie de tasques transversals per dotar de coherència i integritat a totes les funcions executades a l'Agència:

- Mantenir actualitzada tota la informació relativa al risc i a la seva gestió en el Sistema de Gestió del Risc que proporcioni l'Agència.
- Participar en el model de relació amb els clients i proveïdors de l'Agència, involucrant-se amb ells segons les necessitats de seguretat, els informes de seguiment requerits i les tipologies d'activitat.
- Gestionar les reunions i els conflictes que puguin aparèixer durant l'execució de les tasques.
- Generar actes de les reunions internes i les realitzades amb tercers, identificant clarament els participants les tasques tractades i els acords assolits.
- Portar a terme els plans d'actuació que facilitin la industrialització de l'activitat, segons el model presentat pel licitador a la seva proposta i segons la planificació pactada amb la Direcció de l'Agència.
- Mantenir una comunicació fluida amb l'adjudicatari del Lot 1 del present plec i els serveis i àrees de l'Agència.
- Mantenir un estret contacte amb l'àrea de comunicació de l'Agència per tal de proveir-los del material generat amb cada producte del servei per fer-ne difusió.
- Preservar la relació amb Governança del Risc Corporatiu de l'Agència per tal d'identificar possibles noves amenaces a contemplar als programes de seguretat dels Departaments de la Generalitat de Catalunya.
- Alineació i orientació dels projectes per a la consecució dels objectius estratègics de l'Agència.
- Realitzar, d'acord amb la Direcció de l'àrea d'ESG, un pla d'actuació bimensual amb les tasques planificades per les diferents iniciatives d'evolució o transformació per la pròpia operació del servei.

- Planificar recursos addicionals per donar resposta puntual a pics elevats de feina, si és requerit.
- Definir i gestionar el pla de capacitat del servei.
- Generar els indicadors, informes d'activitat i mètriques de l'activitat del servei.
- Mantenir actualitzada tota la informació i documentació relativa al propi servei i a la seva gestió, en la plataforma de gestió de la documentació que determini l'Agència (Confluence i/o Servidor de Fitxers).
- Proposar millores, mantenir i, si s'escau, construir les metodologies pròpies de treball dels serveis objecte de licitació.

3.1 Condicions d'execució

3.1.2 Horaris

Els serveis s'hauran de desenvolupar d'acord amb els horaris de servei de l'Agència. Es consideren horaris laborables els que corresponguin al centre de treball de l'Hospitalet de Llobregat i estiguin prèviament pactats amb l'àrea d'ESG, i l'horari orientatiu està entre les 9:00h i les 18:00h. S'espera que el servei cobreixi les vacances i els períodes de baixa productivitat amb els mateixos integrants establint torns per tal de mantenir uns serveis mínims.

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

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

3.1.3 Localització física

En condicions de normalitat, l'equip prestatari del servei haurà d'estar instal·lat físicament a les oficines de l'Agència, ubicada a l'Hospitalet de Llobregat. En aquest context, l'Agència pot requerir de forma puntual el desplaçament de recursos a altres instal·lacions pertanyents a clients i/o proveïdors de l'Agència. En cap cas la ubicació dels professionals suposarà un increment dels costos vinculats a la prestació dels serveis.

Sota petició expressa de l'Agència o per mitjà d'una proposta dels licitadors, els recursos d'entrada presencials podran substituir-se totalment o parcial per recursos en remot. A la inversa, si durant la prestació en remot l'Agència considera que el servei no està dissenyat correctament, s'implementa ineficaçment o demostra manca de garanties pel fet de no ser presencial, l'Agència pot exigir-lo de forma presencial sense cost afegit.

Tanmateix, ateses les condicions d'excepcionalitat i les directrius de distanciament social establertes per l'Agència motivades per la covid-19, l'adjudicatari haurà de realitzar les seves funcions de forma remota quan sigui requerit. El proveïdor farà una proposta vinculant de prestació remota d'aquest servei que inclourà la metodologia de treball proposada per evitar cap perjudici en la qualitat del desenvolupament del servei.

3.1.4 Rotació de recursos

L'Agència tindrà dret a exigir justificadament a l'adjudicatari el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. 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 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 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.

L'excessiva rotació del personal podrà ser penalitzada per l'Agència (3.2). 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 serà facturable. S'acordarà entre l'adjudicatari i l'Agència el temps estimat de transició per cada substitució que es produeixi, essent el període mínim establert per a la transició de 4 dies laborables.

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

3.1.5 Eines i equipament

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

- Ubicació física adequada per al desenvolupament i prestació del servei, a les instal·lacions de l'Agència.
- Accés a Internet a través de la xarxa local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.
- L'entorn al núvol on s'allotjarà el Bròmetre de Ciberseguretat.

L'Agència no proveirà:

- Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina.
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.
- Ordinadors portàtils (PCs) o altres dispositius mòbils.
- Accés a Internet via comunicacions mòbils.
- Eines per al control de canvis i la gestió de versions.
- Cap altre recurs no especificat explícitament.

En conseqüència, els adjudicataris hauran de:

- Subministrar tots els elements de maquinari, assumir el cost del llicenciament del programari (p. ex. PowerBI) 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 i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.

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

S'ha de realitzar una proposta homogènia de maquinari, programari i de tots aquells accessoris i equipaments auxiliars que siguin necessaris per què els treballadors puguin executar les seves funcions amb eficàcia, disposant d'un entorn adaptat a les necessitats de cada tipus d'usuari. Els equips hauran de seguir les especificacions donades per l'equip de Mitjans Tècnics per garantir la compatibilitat amb el sistema de maquetat i per reduir al mínim el nombre de maquetes necessàries pel servei de Suport al Lloc de Treball.

L'equip portàtil o de sobretaula que l'adjudicatari posi a disposició de l'equip del servei, haurà d'estar maquetat per l'Agència amb el programari i les llicències que l'adjudicatari proporcioni. Per facilitar la gestió, l'Agència posa a disposició de l'adjudicatari la possibilitat d'utilitzar la maqueta pròpia de l'Agència, assumint el mateix adjudicatari els costos de llicenciament del programari (sistema operatiu, suite office, antivirus, PowerBI, etc.).

L'Agència es troba en un procés de revisió i millora contínua que pot implicar la realització de canvis importants en el referent a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei. Per aquest motiu és imprescindible que l'adjudicatari tingui presents les següents consideracions en el referent a les eines de gestió durant l'execució del contracte:

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

3.1.6 Seguretat corporativa

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

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

i controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.

— Els equips, així com la informació resident dels mateixos serà sempre custodiada per l'Agència.

— Garantir l'estabilitat dels equips (reduint al mínim la rotació de personal)

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

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

3.1.7 Control de gestió

El personal del licitador haurà de col·laborar amb l'àrea de Control de Gestió de l'Agència 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.

— Conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència, d'acord amb els procediments establerts.

— Exercir la gestió del contracte amb capacitats de *forecast.*

— Realitzar el *reporting* en les eines proporcionades per l'Agència amb els següents conceptes:

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

L'adjudicatari proporcionarà la seva total col·laboració per a la realització d'auditories i la verificació del compliment dels compromisos. Aquestes auditories, realitzades en qualsevol de les instal·lacions involucrades en la prestació del servei, podran ser portades a terme per personal de l'Agència o sol·licitades a tercers. No serà necessari fer una notificació prèvia per a la realització de tasques d'auditoria que no requereixin la col·laboració activa per part del personal de l'adjudicatari. En el cas en què sigui necessària aquesta col·laboració, l'Agència farà una notificació amb dues setmanes d'antelació. L'adjudicatari suportarà els costos d'auditories adjudicades a tercers i gestionades per la Fundació, destinant al seu finançament un màxim del 0.7% de l'import anual dels serveis contractats.

3.1.8 Validació de la documentació

L'Agència és el propietari de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris i el seu personal i subcontractats que destini a l'execució dels

serveis. L'adjudicatari s'encarregarà de disposar de totes les autoritzacions i permisos necessaris per tal de poder donar compliment a aquesta previsió, essent responsabilitat de l'adjudicatari qualsevol pagament o reclamació relativa a aquesta manca d'autoritzacions.

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

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

3.1.9 Formació

El personal de l'adjudicatari disposarà de la formació adequada per al desenvolupament de les seves tasques. Sens perjudici d'aquesta qüestió el personal de l'adjudicatari realitzarà, si s'escau, formació continuada per tal de garantir l'actualització dels seus coneixements així com l'adquisició de nou coneixement que pugui ser de valor pels serveis de l'Agència. L'adjudicatari haurà de reservar un 5% del temps del personal per tasques de formació i certificació (en matèries relacionades amb l'activitat del contracte) i aquest temps no serà facturat a l'Agència, valorant-se la disposició d'un pla de formació per al personal de l'adjudicatari destinat a l'Agència. Aquest pla es coordinarà amb les activitats i accions de formació pròpies de l'Agència.

3.2 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 doni compliment als present plec i a les prescripcions del contracte.

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

El model de penalitzacions que s'aplicaran per l'incompliment dels indicadors i Acords de Nivell de Servei (ANS) definits, d'acord amb els criteris, quantificació i mètode de càlcul són els establerts a la clàusula 26 del Plec de Clàusules Administratives Particulars.

3.3 Indicadors i acords de nivell de servei

Tipus	Nom	Descripció	Formula de càlcul / Eines	Periodicitat	Llindar Inicial (Li)	Llindar Final (Lf)	Penalització Màxima
Personal	Rotació de personal	Índex de rotació del personal presencial en el servei	Índex de rotació de personal = (((A + D)/2) *100)/ES A = Admissions de personal presencial en el servei dins del període considerat. D = Desvinculacions de personal presencial en el servei dins del període considerat. ES = Número d'efectius del servei segons s'estableix en la proposta de servei pel període considerat; si hagués alguna ampliació del servei en número de recursos humans durant el període considerat, es considerarà el valor ponderat al temps d'aplicabilitat.	Mensual	N/A	N/A	% Índex de Rotació x Import de la factura mensual
Personal	Termini per la reposició de recursos	Termini de substitució d'un recurs per un altre, tant sigui per baixa o per rotació de personal	Dies de desviament respecte el termini de reposició de recursos definit	Per recurs	5 dies	15 dies	Import equivalent a les hores de no disponibilitat del recurs.
Personal	No disponibilitat del personal	L'incompliment de l'horari de servei, la no disponibilitat de servei o la no presència en el lloc de treball en qualsevol moment del període contractat	Hores no disponibles per causes no justificades	Mensual	N/A	N/A	Import de 2h de servei per cada hora de no disponibilitat
Disponibilitat	Nivells de suport en la resposta i resolució d'incidències que afectin a la disponibilitat o qualitat del servei	Retard excessiu en la resposta i resolució d'incidències que afectin a la disponibilitat o qualitat del servei	Hores des de l'avís de la incidència fins que se soluciona	Per incidència	4h	8h	Import de 2h de servei per cada hora de no disponibilitat o qualitat degradada del servei
Qualitat	Qualitat dels lliurables del servei	Grau de satisfacció del client respecte dels indicadors i els informes generats	Puntuació de 1 a 10 segons enquestes de satisfacció al client	Mensual	8	5,5	20% del cost mensual del servei
Lliuraments	Lliurament de l'entorn tecnològic	Desviació en la previsió de disponibilitat productiva de l'entorn tecnològic sobre la previsió	Dies desviats respecte la data establerta del lliurament de l'entorn tecnològic	Mensual	2 dies	30 dies	100% del cost mensual del servei
Lliuraments	Lliurament dels lliurables del servei	Desviació en la previsió dels indicadors de govern del servei	Dies desviats respecte la data establerta del lliurament dels indicadors o altres lliurables	Mensual	2 dies	6 dies	10% del cost mensual del servei
Gestió	Implantació del Model de Reporting	Desviament de temps respecte la data d'entrega del model	Dies desviats respecte la data d'entrega establerta	Mensual	5 dies	15 dies	100% del cost mensual del servei
Devolució	Desviació sobre les tasques per a la devolució	Retard o incompliment dels termes requerits per a la correcta devolució del servei	Dies de desviació	Mensual	2 dies	15 dies	100% del cost mensual del servei

L'Hospitalet de Llobregat, 13 d'octubre de 2020

Oriol Torruella
Director General de l'Agència de Ciberseguretat de Catalunya

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

ANNEX I. Evidències

Llistat de les evidències mínimes que la solució del Lot 1 ha de recollir i avaluar per al càlcul de mètriques i els indicadors del nivell de maduresa en ciberseguretat:

- Activitat sospitosa: comunicacions dirigides a destins sense servei o utilitat aparent, significatiu d'escanejos a la cerca d'altres dispositius a infectar.
- Navegadors compromesos: detecció de navegadors infectats amb *malware* que altera l'experiència de l'usuari.
- Servidors compromesos: servidors que mantenen una activitat maliciosa, com l'allotjament de llocs web de *phishing*, frau o difusió de *malware*.
- Activitat *botnet*: comunicacions realitzades que s'identifiquin com a activitat d'una xarxa de bots, ja sigui d'un bot o un servidor C&C.
- Difusió d'*spam*: enviament de correu brossa des del sistema.
- Compartició de fitxers: transferència de fitxers o programari a través d'un servidor centralitzat (FTP, correu electrònic, missatgeria instantània, etc.), serveis d'emmagatzematge al núvol o xarxes *peer-to-peer* (Bit Torrent, Gnutella, etc.).
- Exposició de credencials: filtració de dades corporatives, com credencials, publicades a la xarxa.
- Incidents de seguretat i fuites d'informació: accessos no desitjats a recursos amb informació restringida d'una organització.
- Dominis SPF: verificació que els dominis disposen de registres SPF assegurar l'autoria legítima dels correus rebuts per evitar l'*email spoofing*.
- Registres DKIM: verificació de l'ús de DKIM per assegurar l'autoria legítima dels correus enviats per evitar l'*email spoofing*.
- Configuracions i certificats TLS/SSL: verificació de l'existència, vigència i configuració de certificats TLS/SSL.
- Ports oberts: detecció de ports oberts innecessàriament que poden facilitar la temptativa d'atacs d'incursió a la xarxa.
- Capçaleres web: anàlisi dels camps de capçalera HTTP en matèria de la seguretat de les peticions i resposta.
- Termini de resolució: temps de resolució de les vulnerabilitats detectades.
- Vulnerabilitats i sistemes insegurs: programari, servidors, terminals o dispositius mòbils obsolets, no actualitzats o que intenten realitzar comunicacions amb dominis web inexistents o no registrats.
- DNSSEC: validació de l'ús del protocol DNSSEC per autenticar els servidors DNS.

- Suplantació web: existència de dominis web similars als utilitzats per una organització i que poden ser utilitzats per suplantar-la.

Les evidències han de disposar recollides han de disposar, quan correspongui, de la següent informació mínima associada:

- Moment en què es va detectar l'activitat per primera vegada.
- Moment en què es va detectar l'activitat per darrera vegada.
- Domini / IP afectat i port associat.
- Domini / IP i port destí de la connexió maliciosa.
- Per als certificats: data d'inici i de caducitat, emissor, descripció del xifrat utilitzat.
- Codi CVE de les vulnerabilitats o, en el seu defecte, codi del fabricant.
- Tipus d'infecció detectada i/o família i variant de *malware* associada.
- Entitat a la qual pertany el host/IP, en el cas que el servei la tingui identificada.
- Informació adient per identificar l'evidència detectada i el seu origen.