AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Servei de suport per al desenvolupament i manteniment d'una font d'informació per mesurar el nivell de ciberseguretat i confiança digital en el teixit social i econòmic de Catalunya: l'Índex de Ciberseguretat

CO.02.2023

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

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

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 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 Presidència 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 de l'Agència, 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.

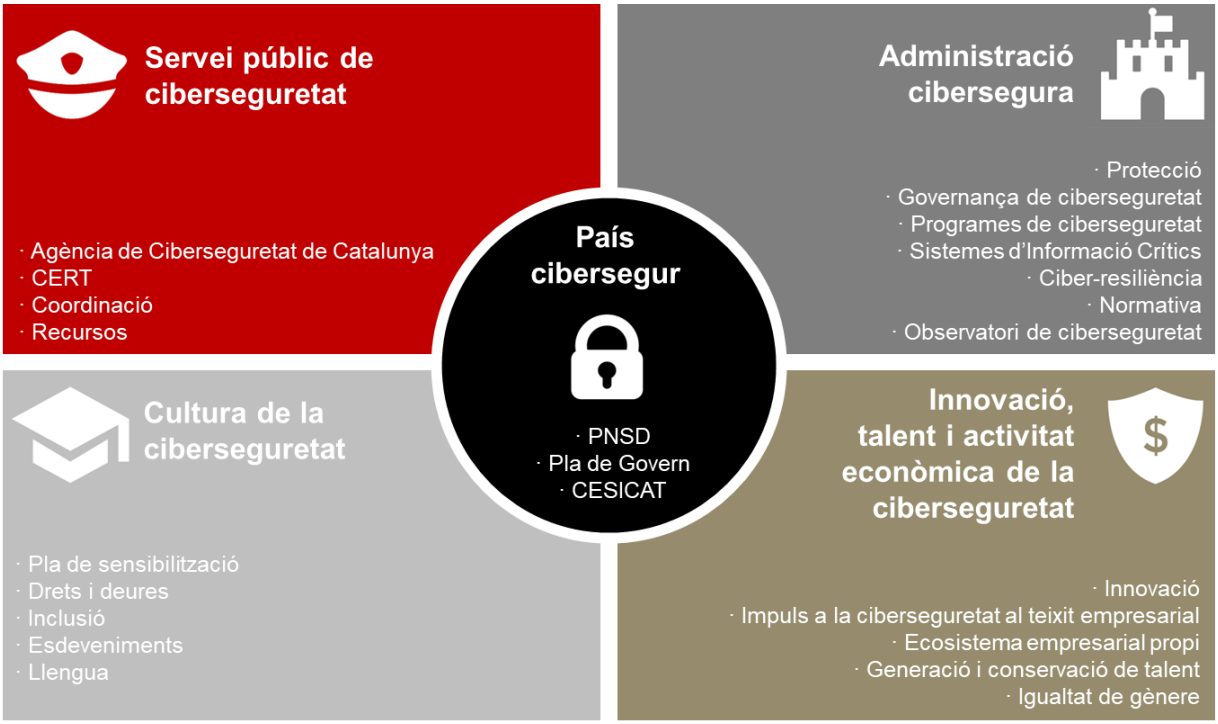
En les funcions que li són pròpies, l'Agència és l'ens idoni per gestionar les tasques necessàries per assolir aquest objectiu de protecció de la informació i la infraestructura TIC de les institucions i ciutadania de Catalunya i, en especial la del Govern de la Generalitat.

1.2 Objectius estratègics

L'Agència de Ciberseguretat de Catalunya neix amb el repte de fer un país cibersegur, i lidera l'Estratègia de Ciberseguretat de la Generalitat de Catalunya 2019-2022, on s'estableix una estratègia operativa de Ciberseguretat basada en la maduresa del govern del risc, fonamentada en l'acció preventiva, en detriment de la reacció com a únic mecanisme de protecció.

L'Agència organitza la seva activitat per mitjà d'un model de governança de la Ciberseguretat des d'on es desenvolupen les funcions de protecció, prevenció i resiliència dels sistemes d'informació i les infraestructures TIC de la Generalitat de Catalunya. Aquestes funcions, juntament amb la de governança de la Ciberseguretat, conformen la cadena de valor de l'entitat amb una clara orientació a la millora de la maduresa en matèria de Ciberseguretat i aportant en tot moment una perspectiva de risc i impacte al negoci.

L'Agència fonamenta la seva activitat estratègica en els següents eixos estratègics:



Eixos d'actuació de l'Estratègia de Ciberseguretat de la Generalitat de Catalunya

— Desplegament d'un Servei Públic de Ciberseguretat executant polítiques públiques.

— Impuls d'una Cultura de Ciberseguretat que permeti assolir una ciutadania digital plena, conscient i capacitada per a l'ús de les TIC i, en especial, en matèria de Ciberseguretat.

— Garant de la Ciberseguretat de l'Administració de la Generalitat de Catalunya i del seu sector públic i de la resta d'entitats i institucions públiques, així com dels ens locals.

— Potencialment del sector econòmic de la Ciberseguretat com a sector estratègic, mitjançant polítiques d'innovació, captació i conservació de talent i dinamització del sector productiu.

En aquest marc estratègic, l'Agència assumeix les funcions d'un Servei públic de Ciberseguretat de la Generalitat de Catalunya, d'entre les quals destaquen:

a) Prevenir i detectar incidents de ciberseguretat i respondre-hi, desplegant les mesures de protecció pertinents.

b) Planificar, gestionar, coordinar i supervisar la ciberseguretat en l'àmbit de l'Administració de la Generalitat i el seu sector públic.

c) Exercir les funcions d'equip de resposta a emergències (CERT) competent a Catalunya.

d) Minimitzar els danys i el temps de recuperació en cas de ciberatac.

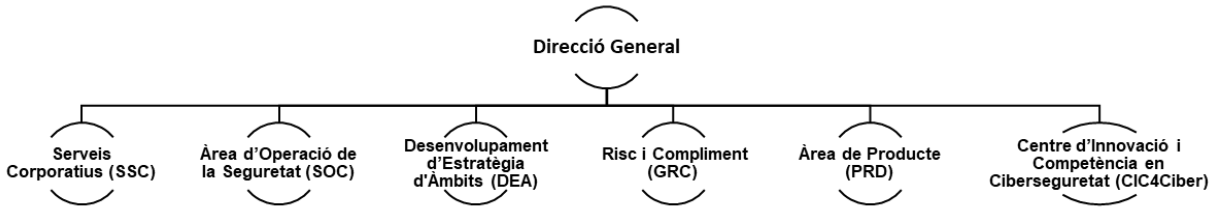
e) Actuar com a suport, en matèria de ciberseguretat, de qualsevol autoritat competent per a l'exercici de les seves funcions públiques.

f) Investigar i analitzar tecnològicament els ciberincidents i ciberatacs.

g) Recollir les dades pertinents de les entitats que gestionen serveis públics o essencials a Catalunya per conèixer l'estat de la seguretat de la informació, informar-ne el Govern i proposar les mesures adequades.

h) Donar suport als responsables de la continuïtat dels serveis i les infraestructures de les tecnologies de la informació i la comunicació de la Generalitat i de les altres administracions públiques que ho requereixin.

1.3 Organització de l'Agència de Ciberseguretat de Catalunya



L'Agència de Ciberseguretat de Catalunya s'organitza en l'estructura següent:

- L'Àrea de Serveis Corporatius (SSC) s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la seguretat corporativa, la comunicació i la gestió de personal.
- L'Àrea d'Operació de la Seguretat (SOC) porta a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, detecció i gestió d'incidents de seguretat en la seva vessant més operativa.
- L'Àrea de Desenvolupament d'Estratègia d'Àmbits (DEA) té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes de Seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- L'Àrea de Risc i Compliment (GRC) es desplega un model de governança que permet coordinar, planificar i adaptar les actuacions en ciberseguretat als riscos propis de cada àmbit, i també és l'encarregada de donar-hi suport a al compliment normatiu i als aspectes legals de la seguretat de la informació.
- L'Àrea de Producte (PRD) s'ocupa d'identificar les necessitats i proposar noves idees i estratègies per a l'elaboració de nous productes generats per l'Agència o millora dels existents, i coordina l'execució del cicle de vida dels productes, des de la seva concepció fins a la seva retirada, incloent el disseny, desenvolupament, desplegament i control de qualitat.

— L'Àrea del Centre d'Innovació i Competència en Ciberseguretat (CIC4Ciber) que es descriu a continuació.

1.4 El Centre d'Innovació i Competència en Ciberseguretat (CIC4Ciber)

El Centre Europeu de Competència Ciberseguretat (ECCC), junt amb la Xarxa de Centres Nacionals (NCC), formen el nou marc d'Europa per recolzar la innovació i la política industrial en ciberseguretat. Són l'estructura de coordinació de la inversió pública europea en ciberseguretat que, aprofitant el que s'ha denominat Comunitat tecnològica de ciberseguretat, establirà una agenda comuna pel desenvolupament i desplegament tecnològic a través de la inversió en projectes estratègics. de ciberseguretat.

És en aquest marc, i per fer aquesta visió una realitat, l'Agència, dins del seu àmbit competencial i territorial, ha creat el CIC4Ciber.

El CIC4Ciber és una estructura organitzativa pública que té un clar objectiu de coordinació, cohesió i capacitació de l'ecosistema de ciberseguretat de Catalunya, es recolza en el coneixement i la innovació com a palanca de transformació i creixement del sector, i en el treball en xarxa com a via per maximitzar l'impacte dels seus programes i projectes, fomentant la captació de fons i la internacionalització.

El CIC4Ciber s'organitza en 4 eixos principals i les seves corresponents línies de servei.

Organització de les línies de servei de l'àrea del CIC4Ciber

1.4.2 Desenvolupament de l' ecosistema.

El CIC4Ciber és un *hub* per oferir una col·laboració pública en ciberseguretat al teixit empresarial cibernètic de Catalunya, així com al sector públic, tals com la finançament d'iniciatives locals i internacionals i la transferència de coneixement. Per aquest motiu, treballa en xarxa identificant sinergies i generant aliances amb socis estratègics a tots els nivells, i localitzant i movent el talent per atraure finançament i definir una agenda d'inversió en innovació en ciberseguretat.

El CIC4Ciber participa en l'ecosistema aportant coneixement en ciberseguretat, de formes diverses (Projectes, Laboratoris, *CyberAcademy*, *Cyber Ranges*, *DataLabs*) i en diferents verticals, com l'operació de la ciberseguretat, l'e-Salut, l'Administració Pública, les tecnologies 5G, l'*Smart Mobility*, el Big Data i l'IA en l'àmbit de la ciberseguretat.

L'activitat del CIC4Ciber està estretament vinculada i posa tota la seva capacitat a disposició del node d'innovació en ciberseguretat del DIH4CAT. Així mateix, amb l'objectiu de coordinar i enfortir el nivell de ciberseguretat del conjunt del ecosistema empresarial i la seva transformació digital, el CIC4Ciber disposa de l'acompanyament d'ACCIÓ, l'Oficina de

Competitivitat Empresarial de la Generalitat de Catalunya, així com les entitats de col·laboració públic-privada, com a la DCA de Catalunya o l'ECSO d'Europa, entre altres entitats col·laboradores.

1.4.3 Innovació

El CIC4Ciber és un element de coordinació de les iniciatives d'acceleració i adopció de la innovació en ciberseguretat a nivell autonòmic. Coordina, cohesiona i estimula l'ecosistema d'innovació en ciberseguretat català amb l'objectiu de revertir, en el propi ecosistema, el coneixement i altres actius generats mitjançant la innovació, per al seu enfortiment. També, p participa en activitats de *brokerage*, on trasllada necessitats i reptes de les àrees operatives de l'Agència, amb rol d'usuari final en projectes d'innovació, col·laborant amb l'ecosistema d'I+D.

Les citades capacitats permeten desenvolupar projectes d'innovació ambiciosos, amb impacte en el territori, fent visible la fortalesa de l'ecosistema català de ciberseguretat en el conjunt de la Unió Europea.

1.4.4 La cultura

El CIC4Ciber desplega l'Acord GOV/143/2018, en el qual s'impulsa el Programa interdepartamental Internet Segura per a la sensibilització i conscienciació de la ciutadania.

S'apropa un gran repte en la provisió de diversitat de perfils de la ciberseguretat: d'operació, gestió, planificació de les organitzacions, i es requereix atraure talent usant tècniques de *reeskilling*, *upskilling*. La Ciberacadèmia del CIC4Ciber, amb visió estratègica sobre capacitats i formació en ciberseguretat, permetrà promoure formacions en activitats laborals específiques i avançades, en coordinació amb les universitats, centres de formació professional o organismes de certificació professional privats. El CIC4Ciber també iniciarà programes que permetin incrementar la presència de dones en posicions de ciberseguretat a Catalunya, i promourà la visió de les oportunitats que té un futur del sector als orientadors dels centres educatius que promouen les STEM.

1.4.5 Ciència i analítica de dades

El desenvolupament de les capacitats de recol·lecció, estructurat i analítica de dades és bàsic per dissenyar estratègies de ciberseguretat *data-driven* d'èxit, i pot suposar un avantatge competitiu essencial que elevi l'activitat del CIC4Ciber a un altre nivell. Tant és així, que a l'hora de prendre decisions, dissenyar estratègies sobre el teixit empresarial o formativa, i implementar la innovació, és fonamental basar-se en dades i informació de qualitat, amb l'objectiu de no haver d'anar a cegues o basant-se en la intuïció. En aquesta línia, l'orientació a la dada permet supervisar la consecució d'objectius i que el model de maduresa del CIC4Ciber està alineat amb les iniciatives i polítiques catalanes, estatals i europees.

Les dades esdevenen cabdals per potenciar les capacitats analítiques i d'intel·ligència, i resulten fonamentals per generar anàlisis de tendències, prospectives, tant globals com sectorials, però sempre des d'una perspectiva ajustada al context i a la realitat de Catalunya. Addicionalment, les dades són un element clau per a la implantació de la Intel·ligència Artificial, la qual arribarà tan lluny com aquestes dades permetin.

1.5 Context dels serveis objecte de licitació

L'any 2021, l'Agència contractava el "Servei per a la monitorització de la ciberseguretat de Catalunya", el qual requeria una solució que calculés el nivell de ciberseguretat de la infraestructura de la Generalitat de Catalunya i de tot el territori de Catalunya, a partir de la recollida massiva d'evidències representatives d'Internet (com els ciberatacs per infecció amb *malware* o les vulnerabilitats).

Al mateix temps, l'Agència contractava un servei per al "Disseny, desenvolupament, implantació, posada en servei i manteniment de l'Índex de Ciberseguretat de Catalunya". El contracte requeria els recursos necessaris per a la creació de l'Índex de Ciberseguretat de Catalunya:

> "una font d'informació, rigorosa i de referència, per mesurar el nivell de ciberseguretat i confiança digital en el teixit social i econòmic de Catalunya"

L'objectiu del desenvolupament de l'Índex de Ciberseguretat tenia la voluntat de recollir les evidències, mètriques i indicadors proporcionats pel ja citat "Servei per a la monitorització de la ciberseguretat de Catalunya", juntament amb dades d'altres fonts, per construir un repositori d'indicadors de valor estratègic per a la ciberseguretat catalana.

Després de 2 anys, de contracte, el servei pel "Disseny, desenvolupament, implantació, posada en servei manteniment de l'Índex de Ciberseguretat de Catalunya" ha expirat i el present plec té l'objectiu de donar-hi continuïtat. La necessitat segueix completament vigent i l'Agència manté la voluntat de continuar el desenvolupament d'un sistema d'informació que esdevingui una referència en la difusió d'indicadors del nivell de maduresa de la ciberseguretat i la confiança digital a Catalunya.

En aquest moment, l'Índex de Ciberseguretat encara no és públic, però s'han desenvolupat diversos actius que el responsable de la present contractació podrà aprofitar per rellançar l'execució del projecte des d'un punt avançat. Cal, però, que el licitador presti atenció a la situació actual de partida del projecte per poder plantejar l'oferta més ajustada i eficient (veure annex I).

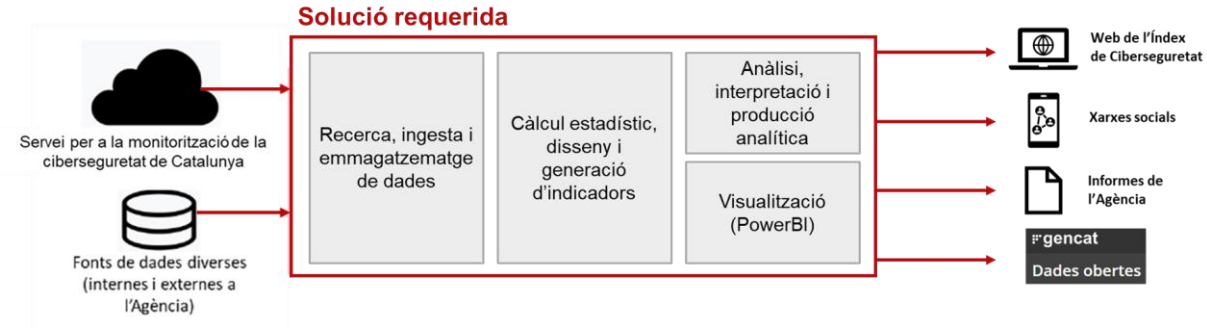
2 DESENVOLUPAMENT I MANTENIMENT DE L'ÍNDEX DE CIBERSEGURETAT DE CATALUNYA

2.1 Objecte

La ràpida evolució de les ciberamenaces requereix una supervisió exhaustiva i continuada, especialment si hi ha la voluntat d'identificar els principals riscos cibernètics, planificar programes de mitigació i fomentar una acció ràpida i efectiva amb l'objectiu de millorar la seguretat dels sistemes d'informació i la confiança digitals. En aquest context, el fet de disposar d'un conjunt adequat d'indicadors que representin l'activitat en matèria de ciberseguretat en el territori de Catalunya esdevé cabdal-.

L'Agència requereix la contractació d'un servei que desenvolupi i mantingui un sistema d'informació on s'aglutini, es processi i s'emmagatzemi, la informació provinent de diferents fonts amb l'objectiu de visualitzar un conjunt d'indicadors que descriguin les característiques i evolució de la ciberseguretat a Catalunya de forma entenedora. Resumidament: en la present licitació, es busca constituir un centre d'operació i anàlisi de dades, encarregat del desplegament i manteniment de l'Índex de Ciberseguretat de Catalunya.

L'Índex de Ciberseguretat esdevindrà una font pública d'informació, rigorosa i de referència, per identificar l'evolució, els punts de millora i els reptes i oportunitats en matèria de ciberseguretat en el territori català. Els sistemes d'informació que conformen l'Índex de Ciberseguretat estaran orientats a identificar, recopilar, emmagatzemar, explotar i difondre les dades necessàries per supervisar, de forma contínua i objectiva, la maduresa en ciberseguretat i el nivell de confiança digital a Catalunya,.



Esquema conceptual de la integració del servei requerit

L'Índex de Ciberseguretat dona resposta a un objectiu estratègic de llarg recorregut, ja que l'adjudicatari tindrà per endavant la tasca d'identificar la informació necessària i explorar noves maneres d'analitzar-la amb l'objectiu d'ampliar i millorar els resultats de forma continuada.

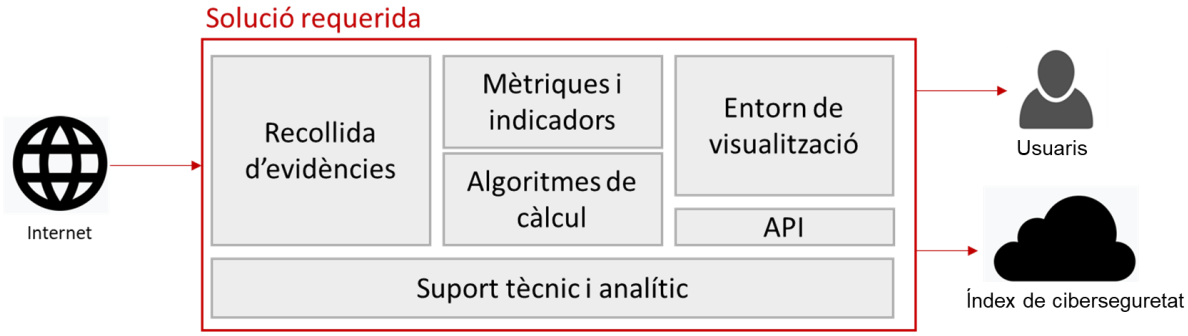
2.2 Antecedents

L'Agència disposa d'una plataforma (actualment del fabricant Bitsight) que recull d'Internet, i de forma continuada en el temps, diferents evidències (*findings*) en matèria de ciberseguretat: infeccions amb *malware*, les vulnerabilitats, els ports oberts, el comportament dels usuaris... del territori de Catalunya. Addicionalment, els indicadors obtinguts s'utilitzen per al càlcul d'una puntuació representativa del nivell de ciberseguretat (*rating*) a partir d'un algoritme objectiu i

explicable. La mateixa plataforma proporciona les evidències, juntament amb el càlcul del *rating* i altres indicadors, a tres nivells diferents:

- El territori de Catalunya.
- La Generalitat de Catalunya.
- Altres entitats.

Part d'aquestes dades són capturades i emmagatzemades per l'Índex de Ciberseguretat a través d'una API, de manera que el sistema d'informació resultant ofereix a l'Agència la capacitat d'utilitzar aquestes dades en combinació amb d'altres de diferents fonts. El sistema resultant es descriu a l'annex I.



Esquema conceptual del servei per a la monitorització de la ciberseguretat de Catalunya

2.3 Objectius del Servei

- Dissenyar i mantenir un conjunt d'indicadors representatius del nivell de maduresa en ciberseguretat i de la confiança digital a Catalunya. Aquests han de permetre:
  - Identificar les principals amenaces de ciberseguretat que poden tenir impacte en la ciutadania i el teixit productiu a Catalunya.
  - Representar, tant a nivell nacional com internacional, les principals iniciatives i assoliments de la ciberseguretat a Catalunya.
  - Avaluar l'impacte de les iniciatives promogudes des de l'Agència (p. ex. plans de comunicació i conscienciació) sobre el nivell de maduresa en matèria de ciberseguretat i la confiança digital de la societat catalana.
  - Identificar activitats, capacitats, necessitats i oportunitats per al sector de la ciberseguretat a Catalunya.
  - 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.).
  - Facilitar el càlcul del Global Cybersecurity Index (GCI) de la ITU de forma continuada en el temps.
- Els indicadors desenvolupats:
  - Han de descriure la ciberseguretat des d'una perspectiva social, tecnològica i econòmica.
  - Sempre que sigui possible, han de disposar de dimensions temporal, geogràfica i sectorial.

- Han d'estar definits i generats amb criteris estadístics provats i rigorosos.

— Per a cada indicador cal:

- Definir la font d'informació d'interès d'on obtenir les mètriques necessàries per al càlcul de l'indicador (p. ex. CSIRT sectorials, APC (Administració Pública Catalana), IdesCAT, Agència Catalana de Consum, Institut d'Estudis de la Seguretat, Universitats i Centres de Recerca, empreses privades, etc.).
- Desenvolupar i mantenir el procés de recollida, ingesta, càlcul estadístic i emmagatzematge més adequat segons el format de les dades i el model de base de dades que garanteixi la seva explotació.

— Difondre els indicadors obtinguts per arribar als destinataris objectiu de forma ràpida i efectiva a través de:

- El sistema de *business intelligence* emprat com a repositori d'indicadors de l'Agència (actualment Power BI) o una solució alternativa degudament justificada.
- El web de l'Índex de Ciberseguretat o altres canals de comunicació propis de l'Agència, com el seu web i xarxes socials.
- El Portal de Dades Obertes de la Generalitat de Catalunya.
- API o a través dels canals d'entitats col·laboradores.
- Recollits en informes elaborats per altres serveis de l'Agència.

— Desenvolupar capacitats operatives per implementar eficaçment les consultes de dades i l'anàlisi estadístic necessaris per donar resposta a peticions o consultes provinents d'altres serveis de l'Agència.

2.4 Activitats del Servei

2.4.1 Disseny i implementació de la plataforma tecnològica al núvol

L'Agència disposa d'una plataforma de l'Índex de Ciberseguretat parcialment construïda en el marc d'un contracte previ. S'ha buscat utilitzar eines individuals, compatibles i integrables amb mòduls estàndard per facilitar la continuïtat del desenvolupament (veure annex I).

D'entrada, l'adjudicatari serà responsable d'analitzar la solució actual desplegada i, si s'escau, dissenyar una aproximació d'arquitectura, software i model de dades diferent, justificant les millores que s'obtindrien, sempre de forma alineada amb els següents aspectes:

— Es dissenyaran i es mantindran els mòduls d'ingesta i processament de dades de fonts diverses, el mòdul d'emmagatzematge i el mòdul de visualització.

— S'utilitzarà l'entorn *cloud* corporatiu sota les condicions del contracte marc vigent del Centre de Telecomunicacions i Tecnologies de la Informació (CTTI), que en l'actualitat és Azure.

— El sistema serà la base de possibles evolucions i ampliacions, de manera que haurà d'estar degudament preparat.

— Es garantirà la ingesta de dades d'altres sistemes d'informació existents a l'Agència, com el sistema d'informació corporatiu, l'eina de captura i emmagatzematge de notícies de ciberseguretat des de fonts obertes, el CRM o el sistema d'informació del SOC (*Security Operations Center*) de l'Agència.

— L'entorn haurà de ser dissenyat i configurat de manera segura, de forma alineada amb les recomanacions i polítiques de l'Agència, i l'adjudicatari serà responsable de

testejar-lo per experts en ciberseguretat. Després de canvis rellevants, l'adjudicatari certificarà amb un informe l'anàlisi de ciberseguretat realitzat i les mesures que han de ser aplicades per l'Agència.

2.4.2 Recerca i ingesta de 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, continuada i sistemàtica, realitzarà les tasques següents:

- Cerca de noves fonts d'informació, tan externes com internes, que donin resposta a una necessitats o oportunitats de l'Agència.
- Recollida, validació, preparació, tractament inicial, anàlisi matemàtic-estadístic i generació d'indicadors.
- Actualització periòdica de les dades i manteniment sistemàtic dels indicadors.

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.

Sempre que sigui possible, les dades carregades s'emmagatzemaran amb els següents atributs clarament definits:

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

I s'hauran de generar les metadades per a tota la informació carregada al sistema d'acord amb els estàndards i millors pràctiques definits pels organismes de Governança de la Generalitat de Catalunya. Les metadades esdevindran un element imprescindible per a l'administració de les dades, però també seran consultables des dels quadres de comandament que es publiquin en línia.

A més, diàriament, l'adjudicatari procedirà a la ingesta, processament i emmagatzematge de la informació que la plataforma del "Servei per a la monitorització de la ciberseguretat de Catalunya" subministrarà via API i de forma automatitzada (actualment, la font disponible és del fabricant Bitsight).

- Aquesta càrrega de dades serà prioritària per sobre de qualsevol altra.
- La informació obtinguda via API correspondrà a un seguit de *findings* de ciberseguretat, com evidències i indicadors, obtinguts de la xarxa al territori de Catalunya.

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

2.4.3 Preparació i explotació de dades

L'adjudicatari serà responsable de l'explotació de les dades recollides per tal de dissenyar indicadors significatius que aportin informació amb continuïtat en el temps. A partir d'aquestes dades, l'adjudicatari s'ocuparà del seu anàlisi amb l'objectiu de generar un relat que expliqui, entre d'altres:

- L'evolució de l'estat del nivell de maduresa de la ciberseguretat i del nivell de confiança digital a Catalunya i, si és possible, per demarcacions territorials
- L'impacte dels plans de comunicació i conscienciació sobre el teixit social i econòmic.
- Principals ciberamenaces en àmbits específics: col·lectius d'entre la ciutadania (en especial els de més risc, com la gent gran i els menors d'edat), sectors econòmics, departaments de la Generalitat de Catalunya, etc.
- L'evolució de la implantació d'esquemes de certificació en ciberseguretat.
- La comparació de Catalunya respecte mètriques i indicadors de referència d'altres regions o estats de l'àmbit nacional o internacional.

2.4.4 Visualització gràfica

A partir de les dades emmagatzemades a l'Índex de Ciberseguretat, l'adjudicatari dissenyarà indicadors que tinguin la capacitat de fer visible la situació de la ciberseguretat a Catalunya. L'adjudicatari serà responsable del disseny, càlcul i implementació gràfica dels indicadors.

Actualment, l'Agència disposa de Power BI com a solució corporativa per a la implementació gràfica dels indicadors, de manera que constitueix la solució tecnològica preferent. Qualsevol proposta alternativa haurà de ser degudament justificada i, en tot cas, l'Agència podrà desestimar-la.

L'adjudicatari emprarà els gràfics interactius més encertats per tal de comunicar adequadament el significat de cada indicador:

- Gràfic lineal, circular, de columnes verticals o horitzontals, radial, d'àrees, de dispersió, de bombolles, de rectangles, etc.
- Distribució de probabilitat contínua o discreta.
- Comparativa entre indicadors.
- Contextualització d'un indicador per àmbit (col·lectiu, sector econòmic, departament, etc.) o geografia.
- Mapes estadístics per municipi, comarca o província de Catalunya.
- Promig d'un indicador respecte el nombre d'habitants o nombre de dispositius connectats (adreces IP) de Catalunya.
- Etc.

L'adjudicatari aglutinarà els gràfics i conformarà quadres de comandament per donar sentit contextualitzat a dades de naturalesa complexa, difícils d'entendre separadament. Els quadres de comandament resumiran la informació, centrant-se en allò important que faciliti la identificació de tendències, relacions, anomalies, etc. Però sense perdre l'accés als detalls dels indicadors.

Per facilitar l'exploració de continguts organitzats en diferents nivells de jerarquia i aconseguir una major versatilitat, els quadres de comandament inclouran un arbre de continguts i elements interactius que permetin, sempre que sigui possible:

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

- Mostrar atributs addicionals per contextualitzar la informació (p. ex. anotacions explicatives, dates rellevants d'efemèrides disruptives, etc.).
- Relacionar diferents visualitzacions i, d'aquesta manera, generar interactivitat mútua.

També possibilitaran el filtratge dels indicadors, sempre que sigui possible, amb els següents filtres:

- Tipologia d'indicador.
- Sector d'activitat econòmica.
- Període temporal.
- Àmbit geogràfic (quan la informació estigui degudament georeferenciada).

L'adjudicatari serà responsable que els productes de visualització elaborats tinguin la qualitat adequada, siguin usables i entenedors.

- Analitzarà que les dades generades per assegurar-se que siguin estadísticament vàlides, tinguin rigor i siguin fidels. Això implica verificar que les dades estan correctament recopilades, sense errors o anomalies que puguin afectar la seva qualitat.
- Realitzarà proves d'usabilitat amb usuaris reals per avaluar la comprensibilitat i facilitat de navegació dels gràfics o quadres de comandament. Aquestes proves permetran identificar possibles problemes d'usabilitat i realitzar les adaptacions necessàries per millorar l'experiència de l'usuari.
- Inclourà els elements, anotacions o explicacions que calgui per clarificar el significat dels elements de navegació i de les pròpies dades presentades (com ara botons, enllaços, menús, etiquetes, *tooltips*, etc.).

2.4.5 Analítica de dades

L'Agència crearà i gestionarà el *subweb* de l'Índex de Ciberseguretat de Catalunya. No obstant, l'adjudicatari, com a centre d'operació i anàlisi de dades, serà responsable de l'elaboració de continguts de qualitat, rigorosos i d'interès, per tal de mantenir-lo viu i actual.

- L'adjudicatari mantindrà degudament actualitzats els quadres de comandament (Power BI) accessibles des d'Internet.
- Amb periodicitat quinzenal, l'adjudicatari elaborarà un mínim d'una publicació (*post*) on s'interpretarà alguna troballa de valor analític obtinguda a partir de les dades disponibles a l'Índex de Ciberseguretat. Cada publicació disposarà de:
  - Un titular representatiu.
  - Un mínim de 10 línies explicatives.
  - Un gràfic en PowerBI incrustat.
- Amb periodicitat quinzenal, l'adjudicatari definirà un conjunt d'indicadors destacats que es publicaran a la capçalera del *site* per contextualitzar els visitants:
  - 3 indicadors de l'àmbit social de la ciberseguretat.
  - 3 de l'àmbit tecnològic de la ciberseguretat.
  - 3 de l'econòmic de la ciberseguretat.
- Quan hi hagi una novetat o algun actualització de les dades publicades, l'adjudicatari elaborarà un avís explicatiu a publicar a la web.

L'adjudicatari serà responsable de posar en valor les visualitzacions i elements gràfics generats. Serà proactiu en definir tècniques i estratègies d'explotació dels productes gràfics generats amb l'objectiu de maximitzar la seva distribució i impacte.

- L'adjudicatari proposarà a l'Agència l'ús dels instruments existents a l'Agència per a la difusió de les publicacions de l'Índex: correu electrònic, webs, xarxes socials, etc.
- L'adjudicatari prepararà visualitzacions accessibles només pels treballadors de l'Agència a través dels quadres de comandament (Power BI) publicats al Tenant Corporatiu.
- L'adjudicatari donarà suport esporàdic a altres serveis de l'Agència, proveint els indicadors i gràfics necessàries per a l'elaboració d'informes o donar resposta a necessitats puntuals.
- Un dels elements a potenciar també és el de publicar *datasets* al portal de dades obertes de la Generalitat, que ja té el seu sistema preparat per poder consumir les dades que hi contenen de forma automàtica. Per tant, caldrà analitzar quina és la millor estratègia a l'hora de publicar les dades en funció de la seva criticitat i privacitat.

2.4.6 Manteniment i millora contínua

En paral·lel a aquest contracte, s'estarà construint una plataforma transversal de dades de la Generalitat de Catalunya (en endavant, PTD), que inclourà, entre d'altres, processos d'ETL, govern i emmagatzematge de les dades, *notebooks* per fer analítica avançada, API d'accés, entre d'altres, i que per tant pot esdevenir un eina important pel que fa a l'emmagatzematge i l'explotació de dades de l'Índex de Ciberseguretat[1].

- La majoria de dades de l'Índex de Ciberseguretat poden anar allotjades a aquesta plataforma i l'adjudicatari haurà de tenir flexibilitat per seguir explotant aquestes dades independentment de si hi ha algun tipus de migració d'informació cap a la PTD. Per altra banda, si escau, podrà usar eines i funcionalitats que aportarà aquesta PTD si estan disponibles i en producció.

També, s'estarà construint una plataforma de serveis transversals d'analítica (en endavant, PTA), que té la voluntat de prestar serveis corporatius per realitzar projectes d'intel·ligència artificial o analítica avançada.

- Caldrà que l'adjudicatari conegui de l'existència de la PTD i la PTA quan estiguin disponibles i poder-ne explorar les seves possibilitats.

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

- 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 de Ciberseguretat actualitzat.

1 https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/notice.pscp?reqCode=viewCn&idDoc=168183d64ac2797975925d06fd8363d1

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

Addicionalment, l'adjudicatari s'ocuparà de mantenir degudament actualitzada la documentació del projecte durant la seva evolució i actualitzarà els següents lliurables una vegada al mes:

- Base de dades documental, fitxes o equivalent amb la descripció, càlcul i interpretació dels diferents indicadors generats.
- Documents del model de dades i arquitectura tecnològica de l'Índex de Ciberseguretat.
- Manual d'ús i administració de l'Índex de Ciberseguretat actualitzat amb una periodicitat mínima mensual.
- Diagrama descriptiu de les interrelacions de l'Índex de Ciberseguretat amb les diferents fonts d'informació i consumidors.

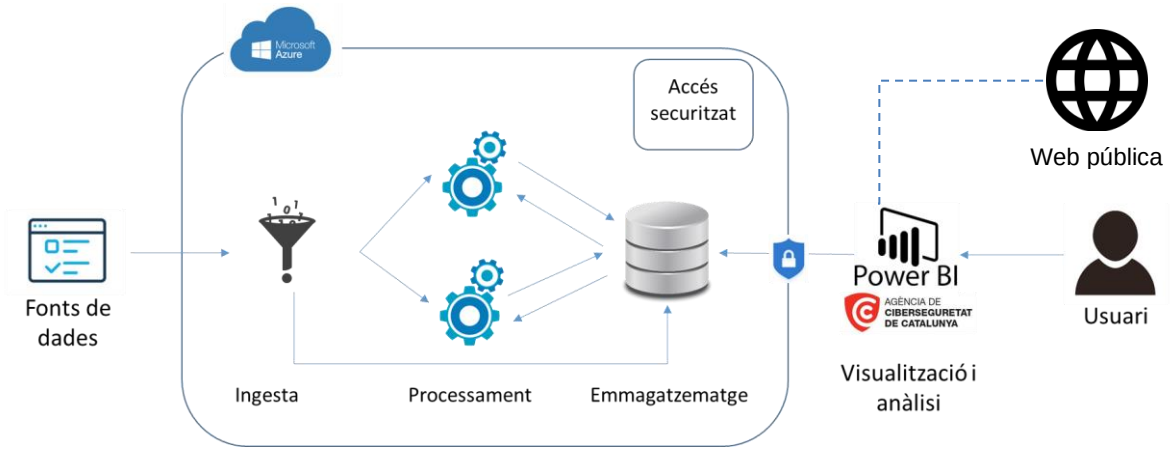
Quan l'Índex de Ciberseguretat estigui en producció, l'adjudicatari realitzarà formació al personal de l'Agència per al seu coneixement, ús i aprofitament. Així mateix, l'Agència podrà sol·licitar posteriors sessions formatives per informar dels evolutius realitzats.

2.5 Requeriments tecnològics de l'Índex de Ciberseguretat

L'Agència disposa d'una plataforma de l'Índex de Ciberseguretat parcialment construïda en el marc d'un contracte de serveis previ a la present licitació. Es basa en la combinació d'un conjunt d'eines individuals, compatibles i integrables amb mòduls estàndard. El licitador haurà de proposar l'arquitectura tecnològica necessària, adaptant-se a les característiques de la solució actual, i tenint en compte que aquesta s'allotja en el núvol d'Azure. El detall de la solució existent actualment es descriu a l'annex I.

En tot cas, a l'inici del contracte, l'adjudicatari analitzarà en profunditat els punts forts i avantatges del desenvolupament actual i planificarà com procedir amb cada component de l'arquitectura. Sempre que es proposi un canvi, aquest haurà de ser justificat, i els nous productes triats hauran de disposar d'un ampli reconeixement i estandardització en el mercat i comptar amb implantacions en el sector públic.

A continuació, es descriu a alt nivell l'arquitectura tecnològica genèrica el servei (el detall de la solució tecnològica desplegada està a l'annex I):



Model esquemàtic d'arquitectura per a l'índex de Ciberseguretat

2.5.1 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.

L'adjudicatari haurà d'estudiar si, addicionalment, és aconsellable implementar una *landing zon*e o *data lake* per emmagatzemar dades en brut, permetent l'accés flexible i exploratori a les mateixes abans de la seva transformació i anàlisis més profunda.

2.5.2 Mòdul d'emmagatzematge

S'haurà de disposar 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.

En funció del volum de dades a carregar i la necessitat de realitzar consultes complexes per a una anàlisi avançada, podrà ser necessari desplegar un emmagatzematge amb arquitectura *big data*.

2.5.3 Mòdul de visualització

El mòdul d'emmagatzematge permetrà preparar les dades per integrar-les amb el mòdul de visualització i permetre el desenvolupament de gràfics i quadres de comandament d'indicadors.

- Es disposarà d'un repositori on es concentraran els gràfics i els quadres de comandaments elaborats.
- Caldrà gestionar els formats adequadament a la seva difusió: obert (per exemple, a la web o webs de determini l'Agència), restringit, intern, etc.
- L'accés als quadres de comandament podrà estar restringit segons el perfil dels diferents usuaris.

2.5.4 Entorns de treball de desenvolupament i producció

L'adjudicatari desplegarà i mantindrà dos 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.

2.5.5 Governança i *DataOps*

La Generalitat de Catalunya té un model per al govern de les dades i cal que les dades de l'Índex de Ciberseguretat segueixin aquest model de govern. Es tracta d'un conjunt de principis i mesures adoptades per una organització per assegurar la fiabilitat, qualitat, disponibilitat i seguretat de les seves dades en tot el cicle de vida .

El licitador proposarà l'ús d'una eina de governança de dades per a garantir la qualitat, la integritat i la conformitat de les mateixes (p. Ex. Informatica, Collibra, Alation, etc.). Aquesta eina haurà de ser compatible amb la resta de tecnologies disponibles a l'Agència i haurà d'oferir funcionalitats per a gestionar i controlar les dades: catalogar, establir polítiques, procediments i estàndards per a la gestió de les dades assegurant que es mantinguin els nivells adequats de qualitat, consistència i seguretat, facilitar la col·laboració entre les part, etc.

El licitador proposarà el desplegament de solucions de *DataOps* que permetin optimitzar i automatitzar eficientment les operacions de dades (p. ex. Jenkins, GitHub, etc.). El licitador haurà de configurar *pipelines* i fluxos de treball per a automatitzar tasques com la ingesta de dades, el processament, l'anàlisi i altres etapes clau de la infraestructura big data. Aquesta automatització estarà orientada a agilitzar els processos i a reduir errors humans, garantint una execució eficient i consistent de les tasques relacionades amb les dades.

2.6 Distribució de l'esforç, perfils mínims i eines del servei

2.6.1 Orientació de la distribució de l'esforç

Els licitadors han de presentar una oferta amb uns recursos que garanteixin la provisió de les activitats del servei segons la següent distribució aproximada d'esforços:

Activitats del servei	Distribució de l'esforç (%)
Disseny i implementació de la plataforma tecnològica al núvol	10%
Recerca i ingesta de fonts d'informació	20%
Preparació i explotació de dades	20%
Visualització gràfica	20%
Analítica de la dades	20%
Manteniment i millora contínua de l'Índex	10%

L'estimació aproximada d'hores efectives anuals necessàries per l'execució dels serveis demanats és de 1,8 FTE anuals (1 FTE té un equivalent a 1.800 hores anuals).

2.6.2 Perfils professionals mínims

Els licitadors hauran d'aportar un equip format pels perfils MÍNIMS que es descriuen a continuació amb l'objectiu de garantir la correcta execució del servei. Ara bé, recau en el licitador el disseny de la proposta de desplegament, la composició de l'equip, la distribució de responsabilitats, l'adequació de perfils i dedicació finals dels mateixos.

Perfil	Requeriments mínims
Consultor especialista en dades	· Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en enginyeria o dades · Experiència mínima de 5 anys en la gestió de projectes de dades
Especialista estadístic	· Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en dades · Experiència mínima de 5 anys en l'elaboració d'estudis estadístics
Enginyer *Big Data*	· Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en enginyeria o dades · Experiència mínima de 5 anys en el desplegament i/o manteniment d'entorns tecnològics de *big data*
Ingestador de dades	· Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en enginyeria · Experiència mínima de 3 anys en projectes relacionats amb la ingesta de dades. · Coneixements tècnics en llibreries de PLN (Processament de Llenguatges Naturals)
Especialista en PowerBI	· Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) · Experiència mínima de 3 anys en disseny d'interfícies i experiències d'usuari en entorns de PowerBI

Expert en Ciberseguretat	· Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en ciberseguretat · Experiència mínima de 5 anys en funcions de ciberseguretat
Especialista en infraestructures cloud	· Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en enginyeria · Experiència mínima de 5 anys com enginyer *cloud* · Coneixement avançat de l'entorn Azure.

2.7 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.

- Núm. de fonts d'informació integrades.
- Volum de dades ingestades.
- Número de *dashboards* generats.
- Núm. de publicacions (posts) a la *subweb* de l'Índex de Ciberseguretat.
- Estadístiques de consulta als quadres de comandament i *site* de l'índex de Ciberseguretat (p. ex. usuaris diaris, informació més consultada...).
- 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.

2.8 Serveis no recurrents

Addicionalment als serveis descrits anteriorment, l'Agència també necessita suport en el desenvolupament de projectes que puguin necessitar un sistema d'informació que aglutini, processi i emmagatzemi dades rellevants per a l'Agència o l'àmbit de la ciberseguretat amb origen en diferents fonts.

Aquesta prestació es durà a terme a criteri de l'Agència en funció de les necessitats en cada cas, i seran considerats serveis no recurrents.

Com a exemples de serveis o projectes que es poden sol·licitar en aquest nivell de prestació són els següents:

- Suport en la recollida, processament i visualització de dades per a diferents àmbits d'actuació (Departaments de la Generalitat les Administracions Locals, l'àmbit de les Infraestructures Essencials i l'àmbit de les Universitats i Centres de Recerca).
- Suport al disseny i/o implantació de tecnologies o processos innovadors, transformació i que permetin millorar i/o renovar l'eficiència de les capacitats de l'Agència en matèria de processat i analítica de dades.
- Suport al disseny /o i implementació de noves interfícies per a la comunicació o visualització de dades i indicadors de ciberseguretat.

No cal fer referència a aquesta tipologia de servei en l'oferta tècnica que presenti cada licitador, i tampoc serà objecte de valoració.

3 ASPECTES GENERALS DE L'EXPEDIENT

3.1 Establiment del servei dins de l'àrea del CIC4Ciber

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 del CIC4Ciber 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.

3.2 Governança del servei

Per realitzar la governança del servei, l'adjudicatari seguirà la metodologia que s'hagi acordat en la fase d'establiment del servei per tal que la gestió de les iniciatives i el seu seguiment siguin àgils, efectius i eficients. El personal de l'adjudicatari reportarà directament als responsables línies de serveis de l'àrea del CIC4Ciber, l'estat, l'evolució i els riscos de les iniciatives o activitats a què dona resposta el servei. Aquest objectius seran mesurables, específics, clars, coherents, realistes i oportuns. D'aquesta manera contribueixen a materialitzar l'estratègia, ajudar a establir les fites i avaluar el compliment, i a crear una alineació de tota l'organització.

La Direcció de l'Agència estableix una sèrie d'objectius a nivell estratègic basades en la visió, missió i valors de l'entitat, i els responsables de línies de servei estableixen quins resultats clau (dos o tres KR, *score*) contribuiran a aquests objectius i a quin equip involucrar per assolir-los. Aquests vindran fixats per una sèrie d'indicadors que permetin mesurar el grau de compliment al llarg del temps dels objectius. Han de ser quantificables, assolibles, comprensibles i no abstractes, expressables en xifres, situats en eix temporal, transformables en iniciatives i activitats específiques i recursos, revisables i qüestionables. Es consensuaran aquests resultats clau (KR) amb l'equip dels adjudicataris i estaran disponibles per l'equip i comunicats adequadament.

Una iniciativa agruparà un conjunt d'activitats orientades a assolir un o més objectius que afectaran els diferents resultats clau associats. Les iniciatives seran inventariades amb la

intenció de prioritzar la seva execució, planificar en el temps el seu abordatge i associar-les als resultats clau als que proporcionen impacte.

Cadascuna de les iniciatives es recolliran en fitxes que responguin la informació següent:

- Quins actius genera?
- A quin ecosistema alimenta?
- A qui cal involucrar?
- Quin finançament cal?
- Els recursos per dur-la a terme estan disponibles?
- Cal realitzar una licitació?
- A quins resultats clau contribueix?
- Genera contingut per a tenir en compte en un pla de comunicació?
- Què està cobert i què cal cobrir?
- Qui té el rol de responsable?
- Té aplicació en un període temporal concret? (identificar l'impacte en el temps l'aportació de valor)
    - Estàndard -execució en un termini raonable-.
    - Atenció immediata -crítica-.
    - Data fixada -si està ben planificada s'evitarà convertir-la d'atenció immediata-.
    - Intangible -es pot allargar en el temps-.

3.3 Metodologia àgil

Les iniciatives es gestionaran amb metodologies àgils i poden aparèixer al *backlog* en qualsevol moment. Tindran un procés de maduració (procés KANBAN) fins que es puguin planificar i incorporar a un trimestre o a un cicle quinzenal: s'han de conceptualitzar, avaluar en termes de viabilitat, esforç, objectius que nodreix, centres de competència que es beneficiaran i classe de servei, etc. Quan la iniciativa està llesta, es pot incorporar a un cicle d'execució.

La descomposició d'iniciatives en tasques detallades es farà el més tard possible. Amb responsabilitat i cura, però el més tard possible. De fet, només es panificarà per a trimestres futurs més enllà del següent trimestre les iniciatives de data fixada.

En aquest sentit, totes les activitats operatives estaran associades a una iniciativa en marxa i tindran un responsable per a la seva execució. Cada activitat es registrarà amb la següent informació:

- Descripció de l'activitat.
- Responsable.
- Data de lliurament.
- Classe de servei.

3.3.1 Planificació trimestral

La fase de planificació esdevé la més important i és on cal dedicar més esforços per a definir els nous resultats clau (KR). Amb l'equip del servei definit, es treballarà en una visió temporal i de preveure necessitats, problemes i riscos per assolir els resultats. Aquesta planificació trimestral s'orienta a aconseguir fites mensuals que s'hagin definit per als resultats claus, perquè així es poden ajustar indicadors quantitatius que s'hagin definit en funció de resultats mensuals. Cada trimestre és focus d'atenció i a trimestres futurs només es fixaran fites conegudes preestablertes com a fitxes de data fixada, la resta és nebulós.

Dues setmanes abans del trimestre en qüestió comença la preparació. Cal avaluar l'assoliment d'objectius, el grau d'avanç de les iniciatives obertes i es prenen decisions respecte als objectius del CIC4Ciber (modificacions, revisió de resultats clau, i fites a assolir, anul·lació, incorporació de nous objectius, etc.). Amb aquest escenari i amb la informació de què es disposa, cal preparar:

- Definició de les iniciatives del trimestre (de les moltes sol·licituds que cal atendre i que estan en el *backlog*).
- Identificació de dates clau.
- Creació de la llista detallada d'iniciatives, especialment les que són ubicables en el temps en una data fixa (termini de presentació, data de celebració, compromís de l'Agència...) i les que tenen dates molt clares ja que la seva finalització condiciona altres equips.
- Identificació de dependències i necessitats i riscos associats al trimestre.
- Estimació de temps per assolir-les i costos.
- Definició del material necessari que cal reservar o adquirir.

Cal tenir en compte les capacitats dels equips, dates i compromisos amb altres equips que requereixen la participació del servei que planifiquem. Aquestes franges de planificació són necessaris a més per coordinacions transversals del CIC4Ciber i de les diferents àrees de l'Agència.

Dues setmanes abans d'acabar el trimestre s'inicia el tancament de l'actual i es prepara planificació del següent.

3.3.2 Seguiment mensual

Es definiran resultats clau per mesurar amb periodicitat mensual l'assoliment quantificable de les fites. Es tracta d'un seguiment àgil permet ajustar les fites mensuals vinculades als KR dels mesos posteriors per orientar-se a assolir els KR trimestrals, a més de adaptar-se als canvis no previstos. En funció de la tendència de compliment de cada mes, es podrà identificar si s'assolirà la fita trimestral,.

- En aquesta avaluació mensual s'observa el progrés, es busquen respostes a preguntes com "estem progressant adequadament?", o "hem de canviar la nostra forma de procedir?", o "hem de cancel·lar determinades iniciatives perquè no estem assolint el que buscàvem?", o "quins experiments hauríem de portar a terme per tal d'aclarir cap a on hem d'anar?".
- La facturació està alineada amb l'acompliment de les fites mensuals, que han de ser lliurables importants, objectius específics o millores planificades. Aquestes fites són els punts de referència per mesurar l'avanç.
- Basant-se en les fites establertes, l'adjudicatari planificarà *sprints* (tindran una durada habitual de 1 a 4 setmanes) durant el qual s'orientarà l'activitat a la realització d'un lliurament de valor.

— Al final de cada *sprint*, es realitza una demostració dels resultats obtinguts i el lliurament que aporta l'increment de valor a l'Agència. La revisió del lliurable de cada *sprint* permet avaluar el treball realitzat, i la validació de l'Agència permet procedir amb la facturació i ajustar les pròximes prioritats i objectius.

— La facturació està directament relacionada amb l'acceptació del lliurament de valor. Cada mes, l'adjudicatari factura per l'esforç dedicat a cada fita assolida i validada per l'Agència. En aquest sentit, per a la facturació, és imprescindible la validació.

3.3.3 Seguiment quinzenal

En reunions de seguiment quinzenal, l'equip posa en comú el grau d'avanç d'activitats que estiguin abordant per tal de conèixer el % de progrés de la iniciativa en curs, ja que les activitats s'associen a una determinada iniciativa.

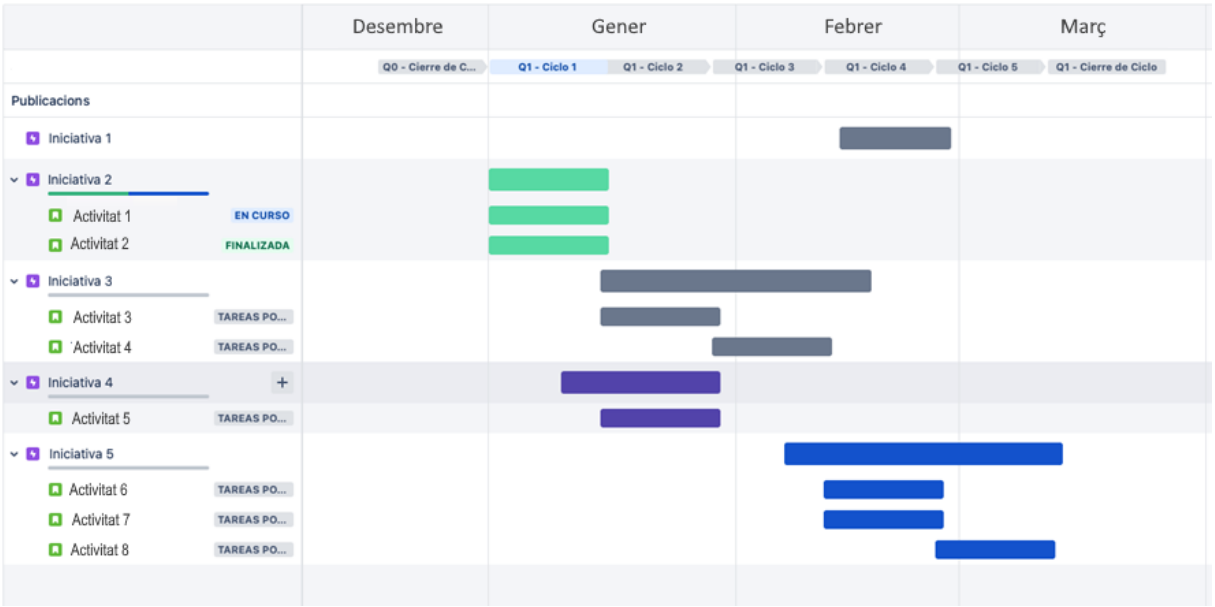
Aquest seguiment consisteix en dues part: una primera (*Review*) on l'equip comparteix i revisa el que s'hagi realitzat en els darrers 15 dies i una segona part (*Planning*) on l'equip planifica les activitats que realitzaran els següents 15 dies. Implementar punts de control abans del seguiment mensual del resultat clau (KR) permet poder incorporar noves activitats a les iniciatives per tal d'apartar-se a noves prioritats i necessitats que puguin sorgir.

Actualitzar els indicadors:

- Número activitats assolides
- Número activitats pendents
- % avanç iniciativa

Es planifica un primer cicle de 15 dies amb les tasques concretes a completar i, en paral·lel a la seva execució, es prepara el cicle següent, identificant necessitats i dependències amb altres equips. Cal assignar tasques de seguiment i persecució dins la rutina diària dels equips, en forma de *check lists* o llistes de control. Altres s'hauran de planificar fora el cicle en curs en data concreta o queden al *backlog* per a cicles a planificar en el futur.

Cal una reflexió sobre els mètodes de treball i millora contínua i planificació del següent cicle.



Mostra de calendari amb iniciatives desglossades amb activitats i degudament programades

3.3.4 Seguiment diari (*Daily*)

Les activitats relacionades amb les iniciatives se seguiran en reunions breus (15 min) de coordinació de l'equip. Es tracta de reunions on participa tot l'equip i on es posa en comú els temes de les activitats que s'estan duent a terme i serveix per avançar, compartir informació i exposar problemes i riscos que puguin sorgir per assolir el compliment de l'activitat.

3.3.5 Posada en comú d'equip

Addicionalment, es fixen punts de trobada i posada en comú per als equips de treball on revisar i reconsiderar les fites que es volen assolir, el seguiment dels resultats clau, les iniciatives i les activitats:

- Per marcar la direcció d'avenç del CIC4Ciber, es porten els equips cap a la mateixa meta i amb enfocament en les prioritats.
- Donar visibilitat sobre l'avenç, tots els involucrats han d'observar l'impacte de les seves tasques en els objectius del CIC4Ciber.
- Identificar colls d'ampolla, detectar falles o obstacles que aturen l'assoliment dels objectius i fomenta la cultura de millora contínua, amb els canals de comunicació comuns i proporcionant transparència del progrés de cada membre en l'equip.

3.4 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.

3.4.1 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.

Alguns serveis contractats són nous, tot i que algunes de les seves funcions podien tenir un procediment d'execució previst des de diferents serveis coexistents i àrees de l'Agència. 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 tasques similars dels serveis. L'adjudicatari haurà de parlar amb els responsables de CIC4Ciber i l'Agència per tal d'entendre el funcionament i la situació actual.
- Adquisició del coneixement de com operar les eines actuals disponibles. L'adjudicatari haurà de recollir les especificacions tècniques i resoldre dubtes dels responsables del servei anterior.
- Adquisició del coneixement del funcionament del servei, les particularitats i de les millors pràctiques. L'adjudicatari haurà de parlar amb els adjudicataris d'altres Contractes per entendre i coordinar el desplegament dels diferents serveis.

3.4.2 Prestació

Es considera la prestació com la fase normal de la prestació del servei. Comença quan els processos d'implantació del nou model 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 (apartat 9) s'han de revisar com a mínim un cop al mes, per tal d'adaptar-los a l'evolució en la prestació dels serveis i a les variacions atenent a les necessitats del CIC4Ciber i l'Agència.

3.4.3 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 generat i desenvolupat, incloent desenvolupaments en Sistemes de la Informació, és propietat de CIC4Ciber i 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 hauran de ser degudament esborrats i tota la informació serà 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.

3.5 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.

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 publicar internament.

El servei de Govern de la Dada és l'encarregat de la realització dels processos de càrrega (ETL), del manteniment i evolució del model de dades i 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 *business intelligence* de l'Agència (Power 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.

3.6 Innovació

En un mon 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.).

3.7 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 del CIC4CIBER, 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 entre els serveis i àrees de l'Agència.
- Mantenir un estret contacte amb el servei 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 del CIC4CIBER, 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.

4 CONDICIONS D'EXECUCIÓ

4.1 Horaris

El servei s'haurà de prestar d'acord amb els horaris de prestació dels serveis de l'Agència, 8x5 en horari de dies laborables. Es considera horari de dies laborables els dies que siguin laborables al centre de treball de l'Hospitalet de Llobregat amb prestació de 9:00h a 18:00h.

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

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

4.2 Localització física

Inicialment, els equips prestataris dels serveis estaran ubicats físicament a les oficines de de l'Agència de Ciberseguretat a l'Hospitalet de Llobregat.

Tanmateix, si les parts així ho acorden l'ajudicatari podrà desenvolupar part dels seus serveis en les seves oficines, atenent sempre a la seguretat de la informació gestionada pel servei. Tot i això, l'Agència considera que l'adjudicatari, en coordinació amb la Direcció de l'àrea de l'Agència, sempre haurà de prestar/executar un mínim del 50% de les tasques/projectes/serveis amb recursos ubicats a les instal·lacions

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

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

4.3 Equip Humà i criteris d'avaluació

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos humans propis que s'aportin i amb la qualificació necessària i adequada per a la prestació del servei.

Els mitjans personals necessaris per a la prestació dels serveis anteriorment indicats han de ser els adequats per realitzar amb garantia les tasques definides i han de mostrar les habilitats necessàries per tal d'integrar-se en un equip d'alt rendiment.

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

S'haurà d'atorgar les responsabilitats pròpies d'un cap de servei a un dels seus recursos, encarregat de dirigir i gestionar la relació del contracte i servei amb l'Agència. Coordinar i fer el seguiment de l'activitat..

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

de fer efectiva en el termini de 15 dies a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència cap 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.

L'excessiva rotació del personal podrà ser penalitzada per l'Agència, segons s'especifica al capítol on es recullen els Acords de Nivell de Servei. 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 2 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.

4.4 Eines i equipament

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

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

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

L'Agència no proveirà:

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

Per aquells serveis que impliquin una prestació continuada i la necessitat d'accedir a a la infraestructura tecnològica de l'Agència, l'Agència proporcionarà a l'adjudicatari:

- Ordinadors portàtils amb el programari habitual de l'Agència per a la prestació del servei.
- Les Eines lligades al lloc de treball necessàries per a la prestació del servei.

Cost mínim orientatiu de la llicencia bàsica i maquinari és de 585.-€ anuals per lloc de treball que es repercutirà a l'adjudicatari. En cas que es requereixin per a la prestació del servei altres llicències no bàsiques, les podrà aportar l'adjudicatari amb el vist-i-plau de l'Agència, o bé proporcionar-les l'entitat, tot compensant els costos que aquest fet generi.

En conseqüència, els adjudicataris hauran de:

- Subministrar tots elements de maquinari, programari i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments de l'objecte del contracte. Aquests elements seran ***d'ús exclusiu*** pels serveis prestats a l'Agència i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.
- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.
- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip de Mitjans Tècnics de l'Agència.

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

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

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

PROPIETAT INTELECTUAL DEL MATERIAL PRODUIT: Cal blindar que l'Agència serà la propietària del material que es produeixi i el proveïdor o proveïdors han de lliurar els documents originals i/o en formats editables de tot el contingut generat pel servei. (redactat formal que caldria afegir-se)

4.5 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.

4.6 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.

4.7 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.

4.8 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.

5 ACORDS DE NIVELL DE SERVEI I PENALITZACIONS

L'adjudicatari resta obligat al compliment de l'execució total de les prestacions recollides en les ofertes que 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 aquest apartat.

A continuació es descriu 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 establerts més endavant, entenent que un mateix fet pot donar lloc a l'aplicació de diferents incompliments i les corresponents penalitzacions d'igual o diferent tipus.

L'import total de les penalitzacions no podrà ser superior al 10% del pressupost anual del contracte. D'acord amb allò establert a l'article 212 de la LCSP la Fundació es reservarà el dret a resoldre el contracte quan el compliment de les diferents prestacions sigui notablement defectuós o assoleixi els llindars de les penalitzacions recollits a la legislació vigent.

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

5.1 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 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

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

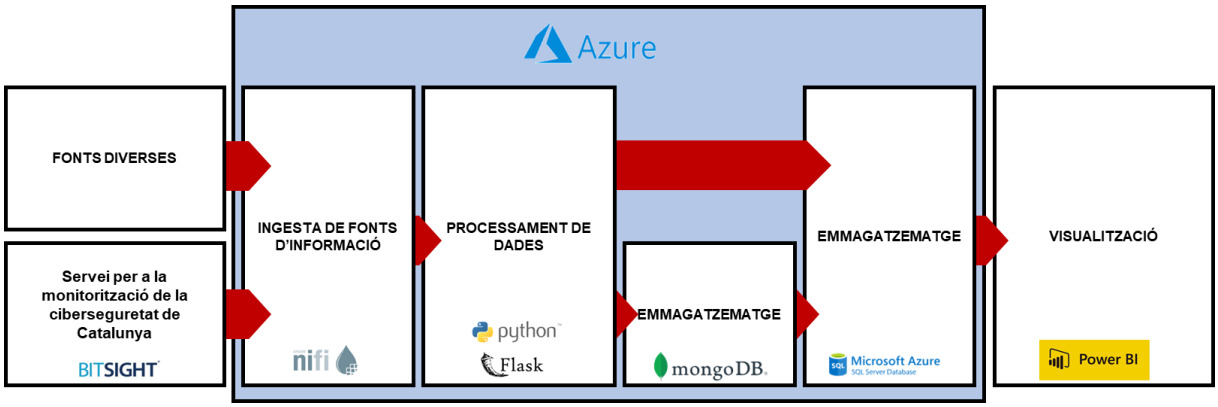
L'Hospitalet de Llobregat, en la data indicada

Isart Canyameres Giménez
Cap d'Unitat d'Innovació

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

ANNEX I. Plataforma actual

A continuació, s'expliquen els serveis que constitueixen la solució desplegada de l'Índex de Ciberseguretat de Catalunya:



Fonts de dades diverses

Algunes dades de diverses fonts d'informació ja disposen d'un procés ETL definit per a seva la ingesta, com per exemple:

- Delictes cibernètics a Catalunya (format: CSV).
- Empreses del sector de la ciberseguretat amb presència a Catalunya (format: CSV).
- Enquestes sobre hàbits de ciberseguretat entre la ciutadania de Catalunya (format: CSV).
- Licitacions adjudicades en matèria de serveis i productes TIC i de ciberseguretat a les administracions públiques catalanes (format: JFON).
- Oferta i demanda de professionals de la ciberseguretat a Catalunya (format: CSV).
- Publicacions ciberseguretat en fonts obertes al món i a Catalunya (format: Solr).

Servei per a la monitorització de la ciberseguretat de Catalunya

Es realitza una càrrega automatitzada de les troballes (*findings*) de ciberseguretat a les xarxes i sistemes d'informació de Catalunya. Aquestes poden consistir en evidències d'infeccions per *malware*, vulnerabilitats, ports oberts i el comportament dels usuaris en l'ús de P2P. En l'actualitat, es fa ús de Bitsight, una plataforma de subscripció que permet mesurar, monitoritzar i investigar els riscos de ciberseguretat de la infraestructura crítica que s'enfronten els territoris.

Mòdul d'ingesta de fonts d'informació

Es fa ús d'Apache NiFi com a solució ETL per a la integració i adquisició de dades des de diferents fonts. El mòdul, dissenyat específicament per gestionar fluxos de dades, permet moure les dades entre diferents sistemes de manera eficient i flexible. S'executa en una

màquina virtual i inclou el seu propi servidor web integrat que ofereix una interfície gràfica per interactuar amb la plataforma

Mòdul de processament de dades

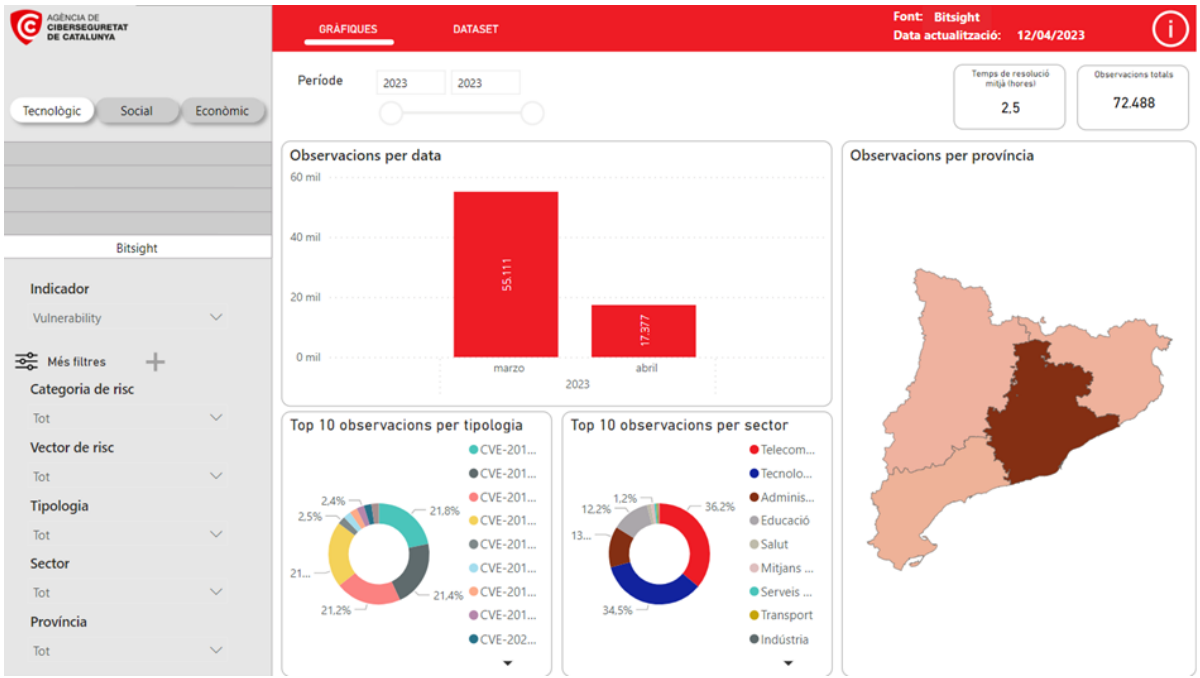
Es fa ús de scripts de Python i Flask per crear microserveis que optimitzin l'estalvi de recursos i l'espai de memòria. El mòdul transforma, normalitza i agrega les dades per a l'anàlisi i la generació de resultats desitjats. El processament de dades implica realitzar aquestes operacions sobre un conjunt determinat de dades, que prèviament han estat emmagatzemades en un repositori d'informació.

Mòdul d'emmagatzematge

Proporciona la capacitat de guardar de manera persistent les dades a la plataforma. Es fa ús d'Azure SQL Database com a solució escalable i fiable per emmagatzemar dades estructurades. En canvi, per a l'emmagatzematge de les dades massives provinents de Bitsight, es disposa d'una base de dades Mongo DB per motius d'eficiència.

Mòdul de visualització

Es disposa d'un conjunt de quadres de comandament, elaborats en Power BI, per a la visualització de les dades.



Captura d'exemple d'un quadre de comandament per a la visualització dels findings de seguretat identificats a Catalunya