MEMÒRIA JUSTIFICATIVA DE CONFORMITAT AMB L'ARTICLE 116 DE LA LCSP ADJUDICACIÓ DIRECTA

L'Objecte de la present memòria és la justificació de les necessitats de l'Agència de Ciberseguretat de Catalunya (en endavant, Agència) per a la formalització d'un contracte per al llicenciament d'una eina que, a partir de la recollida massiva d'evidències d'Internet, subministri el càlcul del nivell de seguretat de les xarxes de Catalunya, l'Administració de la Generalitat i el seu sector públic, administracions locals i altres entitats de Catalunya.

El procediment es durà a terme de conformitat amb el procediment establert en l'apartat 1 de l'annex 9 del plec de clàusules administratives de l'acord marc de serveis de suport a les funcions de Ciberseguretat en matèria d'adquisició i desplegament de solucions de Ciberseguretat per a l'Agència de Ciberseguretat de Catalunya LOT 1 amb número d'expedient AM.05.2024.

OBJECTE DEL CONTRACTE

Objecte: contracte de llicenciament per a una solució que permeti la captura d'evidències i la monitorització del nivell de ciberseguretat al territori de Catalunya i les seves entitats públiques.

L'objecte del present contracte és la contractació d'una solució que, a partir de la recollida massiva d'evidències d'Internet vinculades a diferents factors representatius de la ciberseguretat (com l'existència de vulnerabilitats, males configuracions, infeccions amb *malware*,...), subministri el càlcul del nivell de seguretat de les xarxes de Catalunya i, addicionalment de forma específica, l'Administració de la Generalitat i el seu sector públic, administracions locals i altres entitats 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 fent ús d'un nombre suficient d'evidències, per tal de garantir la seva qualitat i fiabilitat. La solució ha de permetre la monitorització continuada del nivell de ciberseguretat i, a més, facilitar l'accés a les evidències, mètriques i indicadors obtinguts per tal que alimentin de forma automatitzada altres sistemes d'informació de l'Agència.

La solució proposada ha de dotar l'Agència amb la capacitat necessària per recollir les evidències de seguretat i el càlcul del nivell de ciberseguretat a la totalitat del territori de Catalunya i, de forma específica, a un total de 150 entitats.

Tipus: Contracte de serveis

Procediment: Adjudicació directa (annex 9)

CPV:

Pressupost:

Finançat amb Fons Europeus: si. Data d'aprovació del conveni i les entitats. Import total concedit 15.000.000 aportació de INCIBE (75%).

Data conveni: 18 de Desembre de 2023

JUSTIFICACIÓ DE LA CONTRACTACIÓ I NECESSITATS

El present contracte podrà estar finançat fins a un 100% per la Unió Europea NextGenerationUE.

La contractació objecte del present informe resulta necessària per a la realització del compliment i les finalitats institucionals de l'Agència, especialment per a l'acompliment dels objectius.

L'Agència té la consideració d'Administració Pública a efectes de la Llei 9/2017 de Contractes del Sector Públic "LCSP". Sens perjudici d'això, a altres efectes, aquesta entitat resta subjecta al Decret legislatiu 2/2002, de 24 de desembre, pel qual s'aprova el Text refós de la Llei 4/1985, de 29 de març, de l'Estatut de l'Empresa Pública Catalana, sent en conseqüència, una entitat de Dret públic, en general subjecta en la seva activitat al Dret privat.

En un context altament canviant i exigent, en la incorporació de noves capacitats/serveis/recursos/coneixements, com és el món de la ciberseguretat, i més concretament, el món de la ciberseguretat en el context públic, l'Agencia es troba immersa un gran creixement per la qual les licitacions augmenten de manera directament proporcional al creixement de la entitat pública.

Els darrers anys han estat marcats per la pandèmia de la COVID-19, impactant la mateixa fortament en diverses àrees tant del sector privat com del sector públic. Amb motiu de la mateixa es van succeir diversos danys socials i impactes econòmics a aquests sectors que necessiten ésser reparats i recuperats. Aquesta situació va justificar l'aprovació d'un paquet de mesures d'ajut de gran abast pel Consell Europeu en data 21 de juliol de 2020.

Entre aquestes mesures, dins del Pla per la recuperació per Europa, el Consell Europeu va posar en marxa un Instrument Europeu de Recuperació (el programa Next Generation EU) per estimular la recuperació econòmica i la reparació dels danys causats per la pandèmia.

El programa contempla dos instruments financers: (i) El Mecanisme Europeu de Recuperació i Resiliència (en endavant, MRR) i (ii) L'ajuda a la Recuperació per a la Cohesió i els Territoris d'Europa (REACT-UE).

En data 12 de febrer de 2021 es va aprovar el Reglament (UE) 2021/241 del Parlament Europeu i del Consell pel que s'establia el MRR. Norma directament aplicable a tots els estats membres des de la seva publicació al Diari Oficial de la UE.

D'aquesta manera, per poder accedir al MRR, l'estat espanyol va presentar un Pla de Recuperació, Transformació i Resiliència (en endavant, PRTR) aprovat pel Consell de la UE el 13 de juliol de 2021, a on recollia el conjunt d'inversions que es realitzaran i el programa de reformes previstes.

El programa RETECH constitueix un dels nous eixos transversals de l'Agenda España Digital 2026 promoguts pel Ministerio de Asuntos Económicos y Transformación Digital, i està alineat amb dos de les principals fites de l'Agenda, com són, liderar la transformació digital de manera inclusiva i sostenible i focalitzar els esforços de digitalització en sectors econòmics clau. L'objectiu del Programa RETECH és impulsar xarxes territorials d'especialització tecnològica, articulant projectes regionals que

s'orientin a la transformació i especialització digital, assegurant la coordinació la col·laboració i la complementarietat.

Gràcies a aquest nou eix de l'Agenda España Digital 2026, es pretén liderar un canvi disruptiu, de manera inclusiva i sostenible, focalitzant els esforços de digitalització en sectors econòmics clau. En definitiva, la iniciativa RETECH permetrà impulsar els projectes tractors proposats per les Comunitats i Ciutats Autònomes, fomentant l' intercanvi de coneixement i multiplicant les oportunitats de cada regió, a través de xarxes d' impacte nacional que permetin maximitzar l' equilibri territorial i la cohesió social entre elles.

Per fer efectiva la iniciativa RETECH amb total transparència i igualtat d'oportunitats per a totes les Comunitats i Ciutats Autònomes interessades, el Ministerio de Asuntos Económicos i Transformación Digital, a través de la Secretaria d'Estado de Digitalización e Inteligencia Artificial, va llançar una invitació pública destinada al seu desenvolupament de propostes de cooperació per finançar iniciatives emblemàtiques d'especialització territorial tecnològica dins de les seves competències.

El Component 15.I7 (*Ciberseguretat: Enfortiment de les capacitats de Ciberseguretat de ciutadans, pimes i professionals; impuls de l'ecosistema del sector*) és el Component al qual s'ha de contribuir des de l'Agència, i en concret els objectius CID 248 descrits a continuació:

Fita CID 248: Finalització dels projectes dels projectes del programa d'impuls a la indústria de la Ciberseguretat nacional, del programa d'innovació en seguretat i de les accions connexes. Descripció: finalització dels projectes inclosos al Programa d'Impuls a la Indústria de la Ciberseguretat Nacional i al Programa Global d'Innovació en Seguretat, i altres accions connexes en els següents àmbits (adjudicats a la Fita 245 i a la Fita 453): - l'impuls de la indústria de ciberseguretat nacional amb vista al sorgiment, el creixement i el desenvolupament de noves empreses en aquest sector; - el desenvolupament de solucions i serveis d'elevat valor afegit a l'àmbit de la ciberseguretat; - la formació i capacitació de persones amb talent especialitzades en l'àmbit de la ciberseguretat; - les accions d'internacionalització a l'àmbit de la ciberseguretat; - la implantació d'un centre demostrador per al desenvolupament d'infraestructura de ciberseguretat i la creació de nous serveis de ciberseguretat, incloent-hi laboratoris d'assaig i simuladors de ciberatacs; - el desenvolupament de certificacions per a l'etiqueta de ciberseguretat.

Una de les línies d'actuació inclosos en el Pla Operatiu aprovat per INCIBE és el centre demostrador, un projecte dedicat a la investigació i demostració de tecnologies emergents aplicades a la ciberseguretat. L'objectiu principal és avançar en la protecció digital i preparar les empreses i institucions per afrontar els reptes futurs de la ciberseguretat. En aquest sentit, sorgeix la necessitat d'enfortir la capacitat d'avaluar, de manera contínua i objectiva, el nivell de seguretat i el grau d'exposició a les amenaces cibernètiques a les xarxes i sistemes de tot el territori de Catalunya. Aquesta fita esdevé un element clau essencial per obtenir capacitats de resposta i contribuir a la protecció del conjunt de l'ecosistema digital català.

Per tot això, és imprescindible dotar l'Agència d'un mecanisme eficient per a la contractació d'una eina capaç de monitoritzar i calcular el nivell de ciberseguretat a tot Catalunya. En aquesta línia, la present contractació, ha de permetre disposar d'una eina experta per a l'automatització del lliurament de dades, mètriques i indicadors de l'evolució de les amenaces cibernètiques amb abast a tot el territori català. Contribuirà

a reforçar el lideratge institucional en matèria de seguretat digital, augmentar la protecció de la infraestructura tecnològica del país i consolidar la capacitat analítica de l'Agència.

JUSTIFICACIÓ DE LA INSUFICIÈNCIA DE MITJANS

De conformitat amb l'article 30.3 de la LCSP: *"la prestació de serveis es realitzarà normalment per la pròpia Administració pels seus propis mitjans. No obstant, quan no tingui mitjans suficients, prèvia la deguda justificació en l'expedient, es podrà contractar de conformitat amb l'establert al capítol V del títol II del Llibre II de la present Llei"*

En aquest sentit, en l'article 116.4.f) (en concordança amb l'article 63.3.a) LCSP), i en relació amb la necessitat de realitzar la contractació dels serveis objecte del present contracte, l'Agència de Ciberseguretat, posa de manifest la insuficiència de mitjans.

L'Agència no compta amb els coneixements especialitzats ni amb els mitjans tècnics necessaris per desenvolupar i gestionar una eina d'aquest tipus. Aquest és un àmbit d'elevada complexitat que exigeix un accés ampli a fonts de ciberintel·ligència d'abast mundial, el processament de grans quantitats de dades, el disseny d'algoritmes avançats per a l'anàlisi i la correlació d'indicadors, així com les capacitats per garantir una explotació eficient i escalable d'aquestes dades. A més, mantenir la continuïtat, qualitat i fiabilitat de la informació requereix afrontar desafiaments tècnics rellevants, com la normalització de les fonts, la verificació de les evidències recopilades i l'aplicació de criteris homogenis que permetin la comparació dels resultats al llarg del temps.

JUSTIFICACIÓ DEL PROCEDIMENT

En aquest cas, l'adjudicació del contracte s'ha de realitzar de forma directa, ja que l'objecte és l'adquisició de solucions d'un dels fabricants inclosos a l'annex 14 de l'Acord Marc.

L'Acord Marc estableix el procediment per a la compra per adjudicació directa, que es detalla a continuació:

A. Objecte i lots

En l'adjudicació dels contractes basats, tant si es duu a terme de forma directa com mitjançant una nova licitació, cal definir de manera precisa i inequívoca les prestacions a realitzar. Aquestes prestacions estan definides en la memòria justificativa i en l'Annex tècnic.

B. Contractació basada en modalitat de comanda directa

El procediment de contractació per comanda directa s'aplicarà quan l'Agència necessiti la provisió d'una eina de ciberseguretat concreta i identificada d'un dels fabricants inclosos **a l'annex 14.**

L'assignació de comandes directes a les empreses homologades es realitzarà seguint aquestes regles:

- Cada producte a comandar s'assignarà a l'empresa que hagi ofert el millor marge comercial pel fabricant del producte durant el procés d'homologació.
- En cas d'empat entre dues o més empreses amb el mateix marge comercial per fabricant, el producte s'assignarà a l'empresa homologada amb la millor puntuació global en l'homologació.

- Si persisteix l'empat, es considerarà la millor puntuació en el criteri "Elements qualitatius" de l'homologació.
- En cas que l'empat es mantingui, s'aplicaran els criteris de desempat previstos a l'article 147 de la LCSP.

La comanda directa s'assignarà a l'empresa Evolutio cloud en tant és l'empresa que ha ofert marge comercial pel fabricant del producte en el procés d'homologació. L'eina que s'ha de contractar es Bitsight inclosa en l'Annex 14.

L'opció escollida és contractar la llicència per a la solució que proporciona Bitsight, ja que és l'única que permet la monitorització de sistemes d'informació a escala territorial o nacional i a nivell de ciutadania. Bitsight és coneguda per la seva capacitat d'avaluar contínuament la seguretat cibernètica de les organitzacions, proporcionant puntuacions de seguretat que ajuden a identificar i mitigar riscos. També, permetrà la incorporació de la llicència per a la monitorització de 150 organitzacions addicionals, oferint una visibilitat completa i detallada de l'estat de seguretat de cada entitat.

C. Tramitació de la comanda directa

La comanda es tramitarà seguint el model adjunt en el plec de clàusules administratives, incloent-hi les característiques específiques del contracte basat, com els aspectes generals del procediment de contractació, el període contractat, l'import del contracte i les especificitats necessàries per a la provisió. Aquesta informació serà enviada a l'empresa homologada corresponent segons el procediment d'assignació establert.

L'empresa homologada té l'obligació d'acceptar la comanda en un termini de 10 dies hàbils des de la seva recepció, acompanyant-la de la garantia definitiva pertinent. En cas d'incompliment del termini, l'òrgan de contractació aplicarà una penalització del 5% de l'import del contracte basat.

Donat que el contracte està finançat amb fons Next Generation haurà d'aportar la resta de documentació annexa al plec de clàusules administratives.

Si la comanda no és acceptada dins del termini de 10 dies hàbils, es considerarà que l'empresa homologada renuncia a participar en el contracte basat, la qual cosa comportarà la penalització corresponent segons el PCAP. En cas de reiteració, es podria procedir a la resolució de la seva homologació.

La contractació es considerarà formalitzada amb l'acceptació íntegra de la comanda, que no admetrà acceptacions parcials. A més, si el contracte basat implica l'accés o tractament de dades personals, caldrà adjuntar una declaració responsable sobre la ubicació dels servidors que allotgen aquestes dades i des d'on es prestaran els serveis associats. Aquestes declaracions estan incloses en els annexos del plec de clàusules administratives.

Si escau, el contractista haurà d'adjuntar un document de comunicació dels subcontractes a celebrar, especificant la part de la prestació subcontractada, la identitat, les dades de contacte i el representant del subcontractista. A més, haurà de declarar que aquest no està subjecte a cap prohibició de contractació i justificar la seva aptitud per a l'execució del servei, fent constar si la prestació subcontractada inclou la gestió de servidors que allotgin dades personals o serveis associats, indicant-ne la ubicació si escau.

DURADA DEL CONTRACTE

La durada del contracte serà fins al 30 de juny de 2026 a comptar des de la formalització del contracte, de conformitat amb el que estableix l'article 29 de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic (LCSP). Aquesta durada inclou la disponibilitat de la llicència d'ús de la solució tecnològica durant tots els mesos, garantint l'accés continuat a totes les funcionalitats contractades, actualitzacions i manteniment evolutiu de la plataforma.

El conveni de RETECH especifica que el termini d'execució de la despesa conclourà el 30 de juny de 2026 a causa de la seva vinculació als Fons Next Generation, i als objectius i terminis del PRTR, per a aquelles actuacions que estiguin sota el marc del C15.I7

CONSIDERACIONS ECONÒMIQUES

PRESSUPOST DE LICITACIÓ: S'entén per pressupost base de licitació el límit màxim de despesa que en virtut del contracte pot comprometre l'òrgan de contractació, inclòs l'Impost del Valor Afegit, excepte disposició en contrari.

El pressupost base de licitació ascendeix 94.999,51 Euros (IVA exclòs), 114.949,41 Euros (IVA inclòs).

CONSIDERACIONS ECONÒMIQUES

PRESSUPOST DE LICITACIÓ: S'entén per pressupost base de licitació el límit màxim de despesa que en virtut del contracte pot comprometre l'òrgan de contractació, inclòs l'Impost del Valor Afegit, excepte disposició en contrari.

El pressupost base de licitació ascendeix a 114.949,41 Euros (IVA inclòs) amb el següent desglossament:

Concepte	Import en Euros (IVA exclòs)	IVA en Euros (21%)	Import total en Euros (IVA inclòs)
EINA DE CAPTURA D'EVIDÈNCIES I LA MONITORITZACIÓ DEL NIVELL DE CIBERSEGURETAT AL TERRITORI DE CATALUNYA I LES SEVES ENTITATS PÚBLIQUES	94.999,51	19.949,90	114.949,41

Aquest preu s'entendrà com a màxim, l'adjudicació del contracte es farà pel Pressupost Base de licitació de conformitat amb la disposició addicional 33 de la LCSP.

"En los contratos de suministros y de Servicios que tramiten las Administraciones Públicas y demás entidades del sector público con presupuesto limitativo, en los cuales el empresario se obligue a entregar una pluralidad de bienes o a ejecutar el Servicio de forma sucesiva y por precio unitario, sin que el número total de entregas o prestaciones incluidas en el objeto del contrato se defina con exactitud al tiempo de celebrar este, por estar subordinades las mismas a las necesidades de la Administración, deberá aprobarse un presupuesto máximo"

Per a la determinació del pressupost base de licitació s'han tingut en compte els preus de les necessitats que estima l'Agència i tenint en compte la següent taula:

Necessitat per a la captura d'evidències i monitorització del nivell de ciberseguretat	Preu (IVA exclòs)	Preu (IVA inclòs)
Catalunya	64.999,51	78.649,41 €
150 entitats	150 entitats x 200€ = 30.000 €	36.300 €
	94.999,51 €	114.949,41 €

S'ha utilitzat com a referència el preu de 30.000 euros (IVA exclòs) per a la funcionalitat de captura d'evidències i monitorització del nivell de ciberseguretat a les IP del territori de Catalunya, i una estimació segons mercat de 200 euros (IVA exclòs) per a cadascuna de les 150 entitats a monitoritzar.

VALOR ESTIMAT DEL CONTRACTE

S'entén per valor estimat del contracte el valor l'import total, sense incloure l'Impost del Valor Afegit, pagador segons les estimacions realitzades.

El mètode aplicat per calcular el valor estimat del contracte és, de conformitat amb l'article 101 de la LCSP, el següent: Preus de mercat en base a anteriors contractes de l'Agència i d'altres entitats del sector públic.

El valor estimat del contracte ascendeix a la quantitat de 94.999,51 euros (IVA exclòs).

EXISTÈNCIA DE CRÈDIT

Existència de partida pressupostària	Disponible al Capítol 2 de Despesa

S'annexa informe emès pel Director de l'Àrea de Serveis Corporatius on es posa de manifest l'existència de crèdit pressupostària.

QUALIFICACIÓ DE L'OBJECTE DEL CONTRACTE

Es qualifica com un contracte de serveis de conformitat amb el que estableix l'article 17 de la LCSP.

Els contractes de serveis son els que tenen per objecte prestacions consistents en el desenvolupament d'una activitat o que estan adreçats a l'obtenció d'un resultat diferent d'una obra o un subministrament. La LCSP inclou també com a contractes de serveis els contractes en els quals l'adjudicatari s'obliga a executar el servei de manera successiva i per preu unitari.

ALTRES CONSIDERACIONS DEL CONTRACTE

Responsable del contracte

D'acord amb el que estableix l'article 62 de de la LCSP, el responsable del contracte, al qual correspon supervisar-ne l'execució i adoptar les decisions i dictar les instruccions

necessàries amb la finalitat d'assegurar la realització correcta de la prestació pactada.

ALTRES CONSIDERACIONS DEL CONTRACTE

Responsable del contracte

D'acord amb el que estableix l'article 62 de de la LCSP, el responsable del contracte, al qual correspon supervisar-ne l'execució i adoptar les decisions i dictar les instruccions necessàries amb la finalitat d'assegurar la realització correcta de la prestació pactada, dins de l'àmbit de les facultats que l'òrgan de contractació li atribueix serà Jaume Roca, Director de l'Àrea de producte.

De conformitat amb l'article 62 de la LCSP la unitat de seguiment del contracte es determinarà en cada contractació basada essent la direcció d'àrea competent per a cada contracte.

Condicions especials d'execució.

D'acord amb l'article 202 de la LCSP, es mencionen en el present document així com en el Plec de Clàusules Administratives.

a) Condició especial d'execució de caràcter social

Garantir la seguretat i prevenció de la salut en el lloc de treball

b) Condició especial d'execució de caràcter ètic

— Observar els principis, les normes i els cànons ètics propis de les activitats, i professions corresponents a les prestacions objecte del contracte.

— No realitzar accions que posin en risc l'interès públic

— Abstenir-se de realitzar conductes que tinguin per objecte o puguin produir l'efecte d'impedir, restringir o falsejar la competència, com els comportaments col·lusoris o la competència fraudulenta.

— Respectar els acords i les normes de confidencialitat.

— Col·laborar amb l'òrgan de contractació en les actuacions que aquest realitzi pel seguiment i/o avaluació del compliment del contracte, particularment facilitar la informació que li sigui sol·licitada per a aquestes finalitats i que la legislació de transparència i els contractes del sector públic imposen als adjudicataris en relació amb l'Administració o Administracions de referència, sense perjudici del compliment de les obligacions de transparència que els pertoqui de forma directa per previsió legal.

El Reglament 2021/241 del Parlament Europeu i del Consell, de 12 de febrer de 2021, pel qual s'estableix el Mecanisme de Recuperació i Resiliència i la resta de normativa que el desenvolupa, en particular es tindran en compte les mesures que preveu aquest reglament adreçades a:

- El compliment de les fites i objectius segons es disposa a l'annex I de l'ordre HFP/1030/2021, de 29 de setembre.
- L'aplicació dels percentatges de contribució climàtica i digital de les mesures, associats a la inversió 7 del component 15, on s'ha de complir en un 100% a l'etiquetatge digital

- evitar el doble finançament (article 9)
- les mesures contra el frau, la corrupció i el conflicte d'interessos (article 22.2.b)
- les mesures per al registre de les dades dels beneficiaris en una base de dades única (article 22.2.d)
- la subjecció als controls dels organismes europeus (article 22.2.e)
- l'obligació de conservació de la documentació (article 22.2.f)
- les normes sobre comunicació i publicitat, d'acord amb el que preveu l'article 34.

Tanmateix, l'empresa adjudicatària garantirà el respecte al principi de «no causar un perjudici significatiu als objectius medi ambientals» (DNSH), així com el compliment de la metodologia de seguiment de les ajudes d'acord amb el que preveu el PRTR, a l'article 5.2 del Reglament (UE) número 2021/241 del Parlament Europeu i del Consell de data 12 de febrer de 2021, i la seva normativa de desenvolupament i, en particular les vinculades al compliment de fites i objectius.

Revisió de preus

Aquest contracte no està subjecte a revisió de preus.

Termini de garantia

El termini de garantia es determinarà en les posteriors contractacions basades.

Cessió del contracte

De conformitat amb el que estableix l'article 214 de la LCSP, queda prohibida la cessió total o parcial dels drets i obligacions del contractem sense que hi hagi prèviament l'autorització de l'òrgan de contractació i sempre que les qualitats tècniques o personals de qui cedeix no hagin estat raó determinada per a l'adjudicació del contracte.

Penalitats

Les penalitats seran les determinades en l'article 193 de la LCSP, en el present plec de clàusules administratives particulars. En el cas que l'òrgan de contractació ho consideri necessari per l'objecte del contracte, aquestes es concretaran en els posteriors contractes basats prèvia justificació.

S'estableixen les següents penalitats específiques, addicionals a les generals previstes en el PCAP de l'Acord Marc.

- En cas que l'adjudicatari d'una comanda, un cop acceptada i iniciada deixi de servir alguns dels elements, s'aplicarà una penalització del 10% l'import total de la comanda.
- En cas d'incompliment del termini atorgat per a l'acceptació de les comandes directes, l'òrgan de contractació aplicarà una penalització del 5% de l'import del contracte basat.
- En el cas de renunciar a la participació en el contracte basat, l'òrgan de contractació aplicarà una penalització de 10.000 € per cada renúncia.

Annex tècnic

1. Descripció de l'objecte del contracte

1.1. Context del subministrament objecte de la licitació

El servei objecte de licitació en aquest plec està contextualitzat en l'Acord Marc de serveis de suport a les funcions de Ciberseguretat en matèria d'adquisició i desplegament de solucions de Ciberseguretat per a l'Agència de Ciberseguretat de Catalunya amb número d'expedient AM.05.2024, concretament s'emmarca en el lot 1 i el procediment és l'adjudicació directa.

1.2. Objecte i abast del subministrament objecte de la licitació

L'objecte del present contracte és la contractació d'una solució que, a partir de la recollida massiva d'evidències d'Internet vinculades a diferents factors representatius de la ciberseguretat (com l'existència de vulnerabilitats, males configuracions, infeccions amb *malware*,...), subministri el càlcul del nivell de seguretat de les xarxes de Catalunya i, addicionalment de forma específica, l'Administració de la Generalitat i el seu sector públic, administracions locals i altres entitats 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 fent ús d'un nombre suficient d'evidències, per tal de garantir la seva qualitat i fiabilitat. La solució ha de permetre la monitorització continuada del nivell de ciberseguretat i, a més, facilitar l'accés a les evidències, mètriques i indicadors obtinguts per tal que alimentin de forma automatitzada altres sistemes d'informació de l'Agència.

La solució proposada ha de dotar l'Agència amb la capacitat necessària per recollir les evidències de seguretat i el càlcul del nivell de ciberseguretat a la totalitat del territori de Catalunya i, de forma específica, a un total de 150 entitats.

La durada del contracte serà d'un any (1) a comptar des de la formalització del contacte.

1.3. Objectius del subministrament objecte de la licitació

- Obtenir les evidències de ciberseguretat, de forma continuada en el temps, sobre les amenaces, els riscos i els fenòmens de seguretat actuals a nivell de l'Agència, les entitats del sector públic i el conjunt de xarxes de comunicacions electròniques i sistemes d'informació de Catalunya.
- Disposar d'un sistema d'avaluació objectiva de l'estat del nivell de maduresa en matèria de ciberseguretat per a l'Agència, les entitats del sector públic i el conjunt de xarxes de comunicacions electròniques i sistemes d'informació de Catalunya.
- Monitoritzar els indicadors que defineixin el nivell de maduresa en ciberseguretat, a temps real i en base a les evidències recollides, de l'Agència, les entitats del sector públic i el conjunt de xarxes de comunicacions electròniques i sistemes d'informació de Catalunya.
- Disposar d'un sistema d'informació que permeti informar del nivell de maduresa de ciberseguretat a tercers, com la Generalitat i entitats del sector públic de Catalunya.

2. Requeriments tècnics

A continuació es descriuen els serveis, característiques i requisits que conformen l'objecte del contracte. Es tracta d'uns requeriments mínims i necessaris.

2.1. Descripció funcional

2.1.1. 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 del nivell de la seguretat de les seves xarxes de comunicacions electròniques i sistemes d'informació a partir de la recollida d'evidències.

- Recollida d'evidències
  - 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.
  - 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 avaluar, com a mínim, els indicadors de seguretat següents:
    - 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.
    - 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.

- Càlcul del nivell de ciberseguretat

  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 amb un algoritme a partir del conjunt d'evidències recollides.
  - 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 d'activitat econòmica.

2.1.2. Entitats

De forma anàloga a l'apartat anterior, la solució ha de permetre a l'Agència monitoritzar, com a mínim, 150 entitats específiques dins dels seus àmbits competencials. S'hauran d'oferir les característiques següents:

- Ha de permetre l'agrupació d'organitzacions similars per a la creació d'agrupacions de naturalesa similar.
- Addicionalment, ha de permetre a l'Agència monitoritzar la ciberseguretat de la pròpia infraestructura tecnològica.
- Recollida d'evidències i càlcul del nivell de ciberseguretat per entitat (anàlogament a la descripció de l'apartat anterior, però a nivell d'entitat).

2.2. Integració i interoperabilitat

- La solució ha d'oferir serveis d'API (Application Programming Interface) d'accés restringit per a l'Agència que habiliti, de forma segura, la transferència de qualsevol

informació recollida a la solució cap a un altre sistema d'informació, amb l'objectiu de realitzar analítica de dades o la publicació en quadres de comandament.

  - Dades de les troballes, tant a nivell de país com d'entitat.
  - Dades dels indicadors, tant a nivell de país com d'entitat

- Les consultes realitzades a través de l'API permetran capturar les dades de troballes i les seves mètriques per a qualsevol període dins de l'històric de dades disponibles.
  - Més enllà de l'històric disponible, l'Agència podrà sol·licitar el subministrament de dades històriques (prèvies al període d'activació de la solució) de les evidències territorials de Catalunya.

2.3. *Reporting*

La solució proposada disposarà de diferents funcionalitats que permetran la consulta d'informació d'informes automatitzats:

- Generació de quadres de comandament amb els indicadors del nivell de maduresa en matèria de ciberseguretat, els indicadors i les evidències recollides. Aquest nivell de *reporting* es podrà obtenir, tant a nivell del conjunt del territori de Catalunya com per a les entitats monitoritzades.
- Generació d'informes (pdf) de diferent tipologia, més executiva o extensa (en funció de si inclouen el detall de les evidències recollides o no). Aquest informe es podrà obtenir, tant a nivell del conjunt del territori de Catalunya com per a les entitats monitoritzades.

Així mateix, es podran sol·licitar, sota demanda, els següents informes:

- Quadres de comandament interactius del nivell de ciberseguretat de Catalunya en un context global. Aquest informe ha de permetre l'usuari consultar la informació visualment i filtrar, tant per tipologia de troballa com per sector econòmic.
- Informe, de periodicitat anual, sobre el nivell de maduresa en matèria de ciberseguretat per a Catalunya. Aquest informe estarà dirigit a càrrecs directius, de manera que inclourà el significat de les dades i la interpretació dels valors i tendències més rellevants.
- Llistats d'entitats d'àmbits estratègics (p. ex. administracions locals, hospitals, universitats,...) amb la corresponent valoració del *rating* per cadascun dels conceptes.

2.4. 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.

- Sistema de *ticketing* per a la gestió i de peticions i comunicació d'incidències.
- El proveïdor de la solució haurà de gestionar i resoldre les incidències ocorregudes relatives a tot allò que impliqui un funcionament incorrecte de la solució.
- El proveïdor de la solució haurà de resoldre aquelles consultes relacionades amb l'ús, l'administració o la configuració de la solució.

- El proveïdor de la solució 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.
- El proveïdor de la solució oferirà sessions formatives per al personal de l'Agència.
- El proveïdor de la solució oferirà suport haurà d'estar disponible en un horari de 8x5 dins de l'horari d'oficina de l'Agència.
- El proveïdor de la solució disposarà d'un equip per al suport analítica de dades avançada que prestarà suport puntual a l'Agència en quant a la interpretació de les dades o indicadors subministrats..