L'òrgan de contractació de l'Agència de Ciberseguretat de Catalunya, emet la següent memòria justificativa de la contractació

MEMÒRIA

Justificativa de la necessitat i idoneïtat de la contractació dels serveis de "Serveis de suport de l'Àrea de Compliment Normatiu de l'Agència de Ciberseguretat de Catalunya"

De conformitat amb l'article 28 de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic (en endavant, LCSP), la present memòria s'emet als efectes de justificar la naturalesa i extensió de les necessitats que es pretenen cobrir mitjançant el present contracte, així com la idoneïtat del seu objecte i contingut per satisfer-les.

Primer.- Necessitats a satisfer: Les necessitats a satisfer mitjançant el contracte que es pretén licitar consisteixen en:

Lot 1: "Servei d'auditoria"

El servei d'Auditoria és l'encarregat de portar a terme la definició, planificació i execució d'auditories segons l'objecte i abast definits. Integrades dins d'una planificació anual, o invocades sota demanda, les auditories tenen com a finalitat garantir la correcta implementació dels controls definits en el marc normatiu de referència o en les millors pràctiques o entorns normatius en matèria de ciberseguretat.

Concretament, l'Agència duu a terme auditories de compliment normatiu en els següents àmbits:

- Esquema Nacional de Seguretat (ENS).
- Normativa de protecció de dades de caràcter personal de la Generalitat de Catalunya, basada en una metodologia pròpia per a la classificació del risc dels tractaments de dades i un catàleg de mesures de seguretat aplicables als mateixos en virtut de la classificació realitzada, tal i com preveu el RGPD (Marc de Ciberseguretat per a la Protecció de Dades (en endavant, MCPD)), integrat en el Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya (endavant, Marc Normatiu).
- Principals estàndards ISO vigents.
- Altres estàndards de compliment aplicables a la Generalitat de Catalunya.

Potencialment, es podran incorporar altres estàndards que s'aprovin o es determini com a rellevants en l'àmbit de la ciberseguretat a la Generalitat de Catalunya.

D'altra banda, un altre grup rellevant d'auditories que es duen a terme són aquelles auditories relatives al compliment del Marc Normatiu (més informació a l'apartat del servei corresponent). Atenent a les circumstàncies normatives i a l'evolució del model, aquestes auditories tindran una importància creixent per tal de conèixer el nivell de compliment propi del model tecnològic de la Generalitat de Catalunya.

El servei estableix un pla operatiu anual, alineat amb l'estratègia de l'àrea, on es detallen les principals auditories que es preveuen i que d'acord amb la capacitat del servei s'haurien d'assolir. El licitador haurà d'aportar al Responsable de la Línea de Servei (en endavant, RLS) la informació necessària de capacitat i cobertura del servei per a confeccionar el pla anual.

L'Agència disposa de la seva metodologia pròpia per a executar les auditories i per a valorar-ne el resultat, per tant, el licitador l'haurà d'emprar per a prestar els serveis tot aportant-hi aquelles millores operatives que, acordades amb l'RLS, puguin tenir un impacte positiu en el servei.

D'acord amb això, l'Agència precisa de l'execució de les següents tasques:

- Executar els projectes d'auditoria tant d'estàndards de seguretat (basats en el Marc Normatiu elaborat o adoptat per l'Agència, amb les seves actualitzacions i adaptacions especifiques o bé estàndards internacionals de seguretat) com de compliment legal en els marcs legals relatius a la ciberseguretat, principalment, ENS, protecció de dades i ISO, entre d'altres.
- Documentar i presentar els resultats de les auditories d'acord amb el sistema i la metodologia de valoració i de reportat establert al servei i al model de govern del risc de l'Entitat.
- Elaborar i incorporar les mètriques de seguiment del servei i dels resultats de les auditories a les eines corporatives de l'Agència.
- Incorporar i mantenir la informació de les auditories i la relativa al risc i a la seva gestió en el Sistema de Gestió del Risc de l'Agència.
- Emprar l'eina específica de suport operatiu del servei per a dur a terme les auditories, el reportat de mètriques i indicadors de servei i d'activitat.
- Treballar en les millores del procés i documentació de suport del servei i d'altres peticions sota demanda per tal de garantir-ne la màxima eficiència i ajustaments a les necessitats de l'Agència.

Lot 2: "Servei de Marc Normatiu"

El servei de Marc Normatiu es presta des de la Línia de Servei de Marc Normatiu i Auditoria dins l'àrea de Compliment Normatiu de l'Agència.

El desenvolupament del Marc Normatiu es defineix com la creació i manteniment de normes auto-organitzatives derivades de l'ordenament jurídic existent, tant pel que fa a l'àmbit organitzatiu de la Generalitat de Catalunya, com pel que fa a la gestió de la ciberseguretat. És per això, que l'Agència en desenvolupa la funció, en coordinació amb els actors de l'Administració de la Generalitat pertinents, per exemple la Secretaria d'Administració i Funció Pública i el Centre de Telecomunicacions i Tecnologies de la Informació (en endavant, CTTI), i d'acord amb la normativa legal i reglamentària que resulti d'aplicació en cada moment.

El Servei de Marc Normatiu, com eix sobre el qual s'articula el Marc Normatiu, és un servei amb capacitat d'identificació i d'adequació en cada moment a les necessitats concretes de ciberseguretat de la Generalitat de Catalunya.

Així doncs, l'Agència precisa d'un suport que realitzi les següents tasques:

- Mantenir, millorar i evolucionar el Marc Normatiu.
- Donar suport al marc normatiu d'altres interlocutors de l'Administració de la Generalitat de Catalunya (Departaments, organismes i ens), del CTTI i els seus prestadors de serveis TIC, on el Servei de Marc Normatiu hi participa directa o indirectament en la seva elaboració o actualització d'estàndards, per tal d'integrar i incloure aspectes relacionats amb la ciberseguretat.
- Elaborar i actualitzar els diferents estàndards del Marc Normatiu:

  - Documentació de suport (manuals, formularis, plantilles, procediments, etc.)
  - Guies
  - Normes
  - Polítiques
  - Etc.

- Crear nous materials d'acord amb les necessitats manifestades per l'Agència o de manera proactiva, atenent a factors com la tecnologia emprada als seus clients, l'evolució tecnològica, o la urgència en la regulació de determinats fenòmens, entre d'altres.
- Gestió del cicle de vida dels estàndards.
- Publicació dels estàndards a les eines establertes per l'Agència.
- Resolució de consultes i manteniment de la base de dades de coneixement derivada del servei i d'aquestes consultes.
- Integrar el Marc Normatiu amb els models de seguretat i controls preventius, operatius i de gestió presents i futurs.
- Incorporar les mètriques de seguiment i indicadors del servei a les eines corporatives de l'Agència.
- Incorporar i mantenir la informació del Marc Normatiu en el Sistema de Gestió del Risc de l'Agència.
- Treballar en les millores del procés i documentació de suport del servei i d'altres peticions sota demanda per tal de garantir-ne la màxima eficiència i ajustaments a les necessitats de l'Agència.

Lot 3: "Servei de Seguiment de Compliment Normatiu"

El servei de Seguiment de Compliment Normatiu es presta des de la Línia de Servei de Compliment Regulatori i té com a objectiu garantir, a través del seguiment i acompanyament a l'entitat destinataria del servei, el compliment dels principals elements requerits per les normes TIC aplicables, així com el reportat del nivell de compliment assolit. En l'execució d'aquest seguiment s'identifiquen els incompliments i es proposen les solucions pertinents, ja sigui arran de les observacions mostrades en processos d'auditoria o del propi assessorament dels responsables del servei.

Aquesta elaboració de plans i l'execució del seguiment implica la planificació i prestació de les tasques necessàries per a conèixer i reportar periòdicament l'estat de compliment de cadascun dels àmbits en els quals es faci el seguiment (reunions amb

proveïdors, CTTI, amb altres àrees operatives de l'Agència o amb els representants dels Departaments, entre d'altres), així com l'execució d'iniciatives per tal de millorar l'estat de compliment dels plans d'acció. Aquestes iniciatives poden implicar la redacció de documents, el suport i seguiment a processos tècnics o el disseny i implantació de procediments per a donar compliment a exigències normatives. Les mesures a executar les decideix l'RLS, qui definirà l'estratègia de seguiment i analitzarà l'impacte de les mesures, mirant de garantir la màxima eficiència i transversalitat de les actuacions que s'executin des del servei.

En aquest context, l'Agència requereix de suport per a la realització de les següents tasques:

- Definir els plans d'accions necessaris per corregir totes les excepcions i desviacions trobades en els destinatàris del servei durant les auditories o anàlisis prèvies realitzades, ja sigui a través de reunions, entrevistes de l'àrea o a través de l'àrea de Govern del Risc.
- Fer el seguiment d'aquests plans, en col·laboració amb l'àrea de Govern del Risc, amb els destinataris del servei quan correspongui i/o amb els proveïdors implicats i impulsar les accions necessàries pel seu compliment, incloent entre d'altres la redacció de documents, l'assessorament sobre les accions a prendre, l'establiment d'indicadors de criticitat, programes de priorització o la determinació de mesures de seguretat destinades al compliment normatiu.
- Reportar el nivell de compliment normatiu dels diferents entorns on es dugui a terme el seguiment.
- Reportar i mantenir actualitzat el grau de compliment en els sistemes de gestió proporcionats per l'Agència. El reportat dels plans d'acció es realitzarà habitualment de forma bimestral i s'elaboraran els gràfics departamentals amb caràcter semestral, excepte peticions puntuals que es puguin produir per l'RLS o la Direcció d'àrea.
- Elaborar i incorporar les mètriques de seguiment del servei a les eines corporatives de l'Agència.
- Incorporar i mantenir la informació del Seguiment de Compliment Normatiu i la relativa al risc i la seva gestió en el Sistema de Gestió del Risc de l'Agència.
- Fer el seguiment d'aspectes puntuals que puguin sorgir per necessitats normatives específiques.
- Treballar en les millores del procés i documentació de suport del servei i d'altres peticions sota demanda per tal de garantir-ne la màxima eficiència i ajustaments a les necessitats de l'Agència.
- Assessorar sobre les accions a prendre.
- Evolucionar, mantenir, millorar i configurar l'eina desenvolupada a mida per a donar suport operatiu a l'àrea de Compliment Normatiu, concretament al Servei d'Auditoria i al Servei de Seguiment de Compliment Normatiu, incloent la gestió d'usuaris i rols i la construcció de nous indicadors i quadres de comandament per a la visualització de la informació.

Per altra banda, l'Agència contempla també la possibilitat de requerir suport per a executar tasques addicionals que consistiran en la realització de projectes que pretenen la **implementació del MCPD** d'acord amb el projecte d'adequació al Reglament General de Protecció de Dades (en endavant, RGPD), desenvolupat per a la Generalitat de Catalunya, per al Sector Públic substantiu i per aquell que l'Agència decideixi, liderant-ne l'Agència el seu àmbit tecnològic.

Aquestes tasques en les que l'Agència també podria arribar a requerir el suport de l'adjudicatari podran consistir principalment en les següents:

- Suport en la identificació dels tractaments de dades i generació del registre d'activitats de tractament de dades.
- Classificació dels tractaments de dades d'acord amb els criteris definitis en el MCPD.
- Determinació de les mesures de seguretat aplicables, de les definides al MCPD, en funció de la classificació dels tractaments de dades.
- Realització de les Avaluacions d'Impacte relatives a la Protecció de Dades, d'acord amb la metodologia desenvolupada per l'Agència per la Generalitat de Catalunya i el seu sector públic i des de la vessant de la ciberseguretat.
- Identificació inicial del nivell de compliment de les mesures de ciberseguretat del MCPD, en funció de la informació de que disposi l'Agència o de diagnòstics que s'hagin de dur a terme en relació als sistemes d'informació utilitzats pels organismes. Aquesta identificació del nivell de compliment s'haurà de portar a terme de forma que respecti la metodologia establerta per l'Agència.

Aquesta prestació no està sotmesa a l'obligatorietat de la seva realització sinó que s'utilitzarà en funció de les necessitats de l'Agència.

Lot 4: "Servei d'Assessorament Normatiu TIC"

El Servei d'Assessorament Normatiu TIC és un servei d'assessorament legal molt especialitzat en legislació relacionada amb la ciberseguretat. En aquest sentit, es consideren com part d'aquesta legislació, entre d'altres, les normatives que afectin a la seguretat de la informació, la protecció de dades o els mecanismes d'identificació i signatura electrònica.

Aquest servei assessora a les taules, comissions i grups de treball de la Generalitat en les que participa l'Agència, per donar recolzament en aquests aspectes.

Així mateix, el servei també dóna suport d'assessorament legal en matèria de ciberseguretat en els projectes que es porten a terme a l'Agència, principalment des de l'àrea de Govern del Risc, de la pròpia àrea de Compliment Normatiu i de l'entitat. D'igual forma, aquest servei dóna resposta a les necessitats d'assessorament legal pel que fa als projectes en matèria d'identificació i signatura electrònica de la Generalitat de Catalunya i el seu Sector Públic sobre els que hagi de pronunciar-se l'Agència.

El licitador haurà de realitzar les següents tasques segons la modalitat de serveis sol·licitats:

Serveis recurrents

- Donar suport a les taules, comissions i grups de treball de la Generalitat en les que participa l'Agència en el que es refereixi a legislació en matèria de ciberseguretat.

- Gestionar els diferents canals d'entrada de les consultes legals i gestionar els tiquets corresponents a aquest servei mitjançant l'eina de *tiqueting* destinada a l'efecte.
- Establir mecanismes informatius de suport per donar a conèixer novetats legals.
- Analitzar la resposta de les consultes rebudes i els informes jurídics realitzats per tal de determinar la possibilitat d'industrialitzar els continguts més requerits.
- Crear continguts i realitzar accions proactives d'assessorament amb el posicionament de l'entitat d'acord amb la normativa i legislació vigent en matèria de ciberseguretat aplicable a la Generalitat.
- Portar a terme accions de comunicació proactiva d'aspectes rellevants.
- Crear i mantenir un repositori en el que es consolidi el posicionament de l'Agència en les temàtiques més rellevants que s'identifiquin a partir de la resolució de consultes i emisió d'informes jurídics per part del servei.

Així mateix, en funció de les necessitats de l'Agència, existeix la possibilitat de requerir altres tipus de serveis com ara :

- Realitzar informes jurídics que afectin o estiguin relacionats amb les competències de l'Agència. A títol enunciatiu i no limitatiu, a continuació es detallen les temàtiques a tractar en dits informes:

  - Informe d'observacions respecte a la normativa de la Generalitat de Catalunya, o que aquesta hagi de complir, durant la seva elaboració.
  - Informes d'aspectes legals que complementin els relatius a la realització d'análisis de la seguretat i dels riscos d'actius tecnològics dels projectes que porti a terme l'Agència.
  - Informes relatius als aspectes legals que han de complir els mecanismes d'identificació i signatura electrónica.
  - Informes d'assessorament legal en qüestions que es plantegin en el marc de l'activitat de l'Agència, que tinguin alguna implicació en matèria de cibserseguretat i afectació de drets, com els de protecció de dades, intimitat i secret de comunicacions.
- Donar resposta a consultes que afectin o estiguin relacionades amb les competències de l'Agència. A títol enunciatiu i no limitatiu, a continuació es detallen les temàtiques a tractar en dites consultes:

  - Consultes d'assessorament legal sobre mecanismes d'identificació i signatura electrònica i d'altres normatives en matèria de ciberseguretat TIC.
  - Consultes d'assessorament legal a d'altres àrees de l'entitat sobre afectació de drets, com els de protecció de dades, intimitat i secret de comunicacions.
  - Consultes d'assessorament legal a d'altres àrees de l'entitat en relació a la preparació d'escrits, claùsules, contractes i d'altres textos legals, que siguin necessaris per tal de poder complir amb la legislació en matèria de ciberseguretat.

- Mantenir la comunicació amb l'entitat destinataria del servei durant tot el cicle de vida de la consulta legal per a la seva correcta resolució.

Aquesta prestació de serveis no està sotmesa a l'obligatorietat de la seva realització sinó que s'utilitzarà en funció de les necessitats de l'Agència.

Segon.- Objecte del contracte: contractació de Serveis de suport de l'Àrea de Compliment Normatiu de l'Agència de Ciberseguretat de Catalunya i es divideix en quatre lots.

Lot 1: Servei d'auditoria

L'objecte d'aquest lot és portar a terme la definició, planificació i execució d'auditories segons l'objecte i abast definits. Integrades dins d'una planificació anual, o invocades sota demanda, les auditories tenen com a finalitat garantir la correcta implementació dels controls definits en el marc normatiu de referència o en les millors pràctiques o entorns normatius en matèria de ciberseguretat.

Lot 2: Servei de Marc Normatiu

L'objecte d'aquest lot és el desenvolupament del Marc Normatiu, consistent en la creació i manteniment de normes auto-organitzatives derivades de l'ordenament jurídic existent, tant pel que fa a l'àmbit organitzatiu de la Generalitat de Catalunya, com pel que fa a la gestió de la ciberseguretat. Aquesta funció es desenvolupa per l'Agència en coordinació amb els actors de l'Administració de la Generalitat pertinents, per exemple la Secretaria d'Administració i Funció Pública i el Centre de Telecomunicacions i Tecnologies de la Informació (en endavant, CTTI), i d'acord amb la normativa legal i reglamentària que resulti d'aplicació en cada moment.

Lot 3: Servei de seguiment de compliment normatiu

L'objecte d'aquest lot és la prestació del servei deSeguiment de Compliment Normatiu des de la Línia de Servei de Compliment Regulatori i el qual té com a objectiu garantir, a través del seguiment i acompanyament a l'entitat destinatària del servei el compliment dels principals elements requerits per les normes TIC aplicables, així com el reportat del nivell de compliment assolit. En l'execució d'aquest seguiment s'identifiquen els incompliments i es proposen les solucions pertinents, ja sigui arran de les observacions mostrades en processos d'auditoria o del propi assessorament dels responsables del servei.

Lot 4: Servei d'assessorament normatiu TIC

L'objecte d'aquest lot és la prestació del Servei d'Assessorament Normatiu TIC, consistent en l'assessorament legal especialitzat en legislació relacionada amb la ciberseguretat. En aquest sentit, es consideren com part d'aquesta legislació, entre d'altres, les normatives que afectin a la seguretat de la informació, la protecció de dades o els mecanismes d'identificació i signatura electrònica.

Constitueix també l'objecte d'aquest lot l'assessorament a les taules, comissions i grups de treball de la Generalitat en les que participa l'Agència, per donar recolzament en aquests aspectes.

Així mateix, el servei també dóna suport d'assessorament legal en matèria de ciberseguretat en els projectes que es porten a terme a l'Agència, principalment des de l'àrea de Govern del Risc, de la pròpia àrea de Compliment Normatiu i de l'entitat. D'igual forma, aquest servei dóna resposta a les necessitats d'assessorament legal pel que fa als projectes en matèria d'identificació i signatura electrònica de la Generalitat de Catalunya i el seu Sector Públic sobre els que hagi de pronunciar-se l'Agència.

Tercer.- Termini d'execució del contracte: El termini d'execució del contracte per cobrir les necessitats a satisfer es fixa, per tots els lots, en DOTZE (12) mesos, més dues possibles pròrrogues de de DOTZE (12) mesos cadascuna, essent que la durada total del contracte incloses les seves pròrrogues no excedirà de TRENTA-SIS (36) mesos per a cada Lot.

Quart.- Idoneïtat de l'objecte i contingut del contracte: Mitjançant el contracte se satisfaran les necessitats que s'especifiquen en el punt primer de la present memòria, d'acord amb la justificació tècnica que s'adjunta a la present memòria.

Es considera que mitjançant el contracte que es pretén licitar se satisfaran de forma directa, clara i proporcional les necessitats establertes al punt primer de la present memòria.

Cinquè.- Justificació del procediment utilitzat per l'adjudicació del contracte: El contracte s'adjudicarà mitjançant procediment obert, de conformitat amb el que s'estableix a la LCSP, essent necessària la preparació dels plecs de clàusules administratives particulars i de prescripcions tècniques que regeixin la corresponent licitació.

Pels motius exposats es justifica la necessitat i idoneïtat de procedir a la contractació dels esmentats serveis, i a tal efecte,

RESOLC, iniciar el present expedient de contractació.

L'Hospitalet de Llobregat, a 20 d'octubre de 2020

Oriol Torruella Torres
Director General
Agència de Ciberseguretat de Catalunya