PLEC DE PRESCRIPCIONS TÈCNIQUES QUE HAN DE REGIR LA CONTRACTACIÓ D'UNS SERVEIS D'OFICINA TÈCNICA DE SEGURETAT PER DONAR SUPORT A L'AGÈNCIA DE RESIDUS DE CATALUNYA (ARC)

1.- OBJECTE DEL PROCEDIMENT OBERT

L'objecte de la present licitació és la de proporcionar les dades necessàries per a la contractació dels serveis d'una oficina tècnica de seguretat per l'ARC.

La contractació es realitzarà mitjançant un procediment obert i tindrà com objecte el servei d'una oficina tècnica de seguretat.

2.- TERMINI DE LLIURAMENT I DURADA DEL CONTRACTE

El termini d'execució es desglossa de la següent manera: el termini d'inici del servei serà de 2 setmanes a partir de la formalització de l'adjudicació i signatura del contracte.

La durada del contracte serà d'un any, i no s'iniciarà abans de l'1 de gener del 2026 i finalitzarà el 31 de desembre de 2026.

Es preveu que es pugui prorrogar durant 4 anys, amb 4 pròrrogues d'un any, així la duració total màxima del contracte podrà ser, en cas d'executar-se totes les prorrogues, de 5 anys.

Si en algun moment l'Agència de Ciberseguretat de Catalunya (ACC en endavant) ens comunica que ja pot assumir totes les funcions descrites en aquest Plec de Prescripcions Tècniques, es procediria a no renovar la següent pròrroga.

3.- JUSTIFICACIÓ DE LA NECESSITAT I IDONEÏTAT DEL CONTRACTE

La contractació d'una oficina tècnica de seguretat, incloent-hi la figura de CISO ("Chief Information Security Officer"), respon a la necessitat d'assegurar el compliment normatiu i la protecció dels sistemes d'informació, infraestructures essencials i actius digitals de l'organització. L'augment de les ciberamenaces i la creixent regulació en matèria de seguretat i protecció de dades fan imprescindible comptar amb especialistes que puguin dissenyar, implementar i supervisar estratègies de seguretat de manera contínua i eficient, que garanteixin la protecció dels recursos tecnològics i la confidencialitat, integritat i disponibilitat de la informació, sempre de forma coordinada amb l'Agència de Ciberseguretat de Catalunya (ACC).

Altres aspectes rellevants que justifiquen la seva contractació són l'aportació de coneixement especialitzat, flexibilitat i capacitat d'adaptació a noves amenaces. També contribueix a la detecció i resposta ràpida davant incidents, minimitzant l'impacte de possibles vulnerabilitats. Així mateix, facilita la implementació de mesures proactives per a la seguretat de la informació i la protecció d'infraestructures crítiques. En conjunt, aquesta contractació reforça la resiliència de l'organització i garanteix un entorn tecnològic segur i eficient.

4.- DESCRIPCIÓ DE LA SITUACIÓ ACTUAL

L'ARC ja disposa d'un conjunt de mesures de seguretat perimetral per protegir les seves infraestructures, les quals són objecte d'aquest procediment obert. Actualment, l'ARC compta amb:

- EDR Implementat en estacions de treball i servidors per a la detecció i resposta davant amenaces en els endpoints. El centre de control i monitorització ho porta l'ACC, i així ha de continuar.
- Firewall: Utilitzat per a la protecció perimetral de la xarxa, controlant el trànsit d'entrada i sortida.
- WAF: Desplegat per protegir les plataformes web de l'ARC contra atacs específics a aplicacions web.
- Tant el Firewall com el WAF estan allotjats actualment al nostre Centre de Processament de Dades (CPD).
- Autenticació de doble factor: Requerida per a tots els usuaris que accedeixen a les infraestructures, afegint una capa extra de seguretat.

L'ARC està compromesa amb el compliment de l'Esquema Nacional de Seguretat (ENS) en la seva categoria mitja. Això implica, que s'han d'implementar un conjunt de mesures de seguretat específiques per protegir els seus sistemes d'informació i garantir la confidencialitat, integritat i disponibilitat de les dades.

La incorporació d'un/a CISO (Chief Information Security Officer) reforçarà aquestes mesures de seguretat existents i permetrà implementar noves estratègies i tecnologies per assolir un nivell de seguretat òptim. El/la CISO serà responsable de liderar la gestió de la seguretat de la informació, assegurant la protecció dels actius de l'ARC i la conformitat amb les normatives aplicables, sempre amb la coordinació i sota les directrius de l'ACC.

5.- REQUISITS TÈCNICS D'OBLIGAT COMPLIMENT

5.1. Requisits del servei

Els serveis que s'estan sol·licitant han de cobrir tant l'àmbit de la seguretat de la informació com el compliment normatiu durant tot el període de vigència del contracte.

L'Oficina Tècnica de Seguretat estarà integrada per diversos serveis, cadascun amb un àmbit d'actuació, tasques i recursos específics, tal com es detalla a continuació.

5.1.1. Servei de Gestió i Administració de la Seguretat:

a. Haurà d'incloure un perfil que realitzarà les funcions de CISO (Chief Information Security Officer): Que haurà de realitzar la definició i direcció estratègica de la seguretat, a partir de les directrius de l'ACC, realitzar la definició de polítiques i supervisió de les mesures de protecció.
b. Anàlisi i gestió de riscos de seguretat: Identificació d'amenaces, impactes i mesures de mitigació.
c. Creació i gestió de plans directors de seguretat: Desenvolupament i mantenint durant tot el servei un full de ruta per a la millora contínua de la seguretat de la informació.
d. Definir els indicadors de seguretat (KPI/KRI), pel mesurament i control del rendiment de les mesures de seguretat.
e. Col·laborar i donar suport a l'ACC en la definició i implementació de mesures de seguretat, auditoria, resposta a incidents de seguretat i altres accions que puguin ser necessàries per millorar la seguretat i compliment normatiu de l'ARC.
f. Elaboració de plans de contingència i resposta a incidents: Definició de procediments per minimitzar l'impacte d'atacs o fallades alineat amb l'Esquema Nacional de Seguretat (ENS).
g. Auditories de seguretat, amb objectiu de realitzar la verificació de controls establerts, realitzant revisions periòdiques dels plans, directrius i processos de seguretat establerts.
h. Gestió de la continuïtat del negoci (BCP - Business Continuity Plan), dissenyant les mesures necessàries per garantir la disponibilitat dels serveis essencials.

5.1.2 Servei de suport al Compliment Normatiu:

a. Definir, proposar i executar el pla d'adequació a l'Esquema Nacional de Seguretat (ENS), i proporcionar el suport tècnic necessari per realitzar l'adequació de l'ARC.
b. Programar i executar accions de conscienciació i formació per a empleats: Elaboració de documentació per usuaris sobre la seguretat digital i Esquema Nacional de Seguretat.

c. Simulació de phishing i enginyeria social: Campanyes per detectar i reduir el risc d'atacs basats en enganys, per avaluar el nivell de sensibilització dels empleats de l'ARC.

5.1.3 Servei d'Operació de la Seguretat:

a. Donar suport a la supervisió dels sistemes de seguretat de l'ARC per al monitoratge i detecció d'amenaces, integrant les dades i intel·ligència proporcionades per l'ACC per a una detecció i resposta més efectiva d'incidents.
b. Avaluació de vulnerabilitats per millorar la protecció dels sistemes i la realització de tests de penetració (pentesting).
c. Suport a la gestió de vulnerabilitats, bastionat de sistemes i aplicació de mesures per corregir riscos de seguretat.
d. Suport pericial informàtic forense en casos de delictes informàtics, frau, robatori de dades, disputes legals que involucrin evidències digitals, i qualsevol altre cas en què la informació digital sigui rellevant per a la resolució del litigi.
e. Col·laborar i donar suport a l'ACC en la implantació de mesures de seguretat, auditoria, resposta a incidents de seguretat i altres accions que puguin ser necessàries per millorar la seguretat i compliment normatiu de l'ARC.
f. Proves de recuperació i simulacres: Exercicis per comprovar l'eficàcia dels plans de resposta davant incidents.

5.1.4 Altres serveis:

a. S'ha d'incloure un **Servei de Gestió y Suport a la Seguretat,** que permeti gestionar i documentar els incidents de seguretat, segons el que estableix la Guia CCN-STIC 817, basat en una plataforma online, oferint a l'ARC accés continu i informació en temps real a la informació, estat de l'incident, accions realitzades, des de qualsevol ubicació.
b. S'ha d'incloure un **Servei de Vigilància de Seguretat,** basat en una plataforma online, que permeti el monitoratge de l'entorn digital de l'ARC (Vigilància Digital), oferint a l'ARC accés continu i en temps real a la informació des de qualsevol ubicació.
c. S'ha d'incloure un **Servei de Monitoratge** dels indicadors de seguretat**,** que permeti l'actualització automàtica i visualització dels KPI/KRI de seguretat establerts, oferint a l'ARC accés continu i informació en temps real a la informació des de qualsevol ubicació.

Es requereix la presentació d'un pla de treball, detallat que especifiqui les tasques a realitzar durant el primer any. Per als anys successius, el licitador haurà d'elaborar i presentar un nou pla de treball un mes abans de la finalització del període en curs, el qual haurà de ser validat i aprovat per l'ARC. Aquests plans de treball han de cobrir els serveis descrits en aquest plec tècnic i preveure un esforç anual d'entre 750 i 800 hores, incloent una reserva mínima de 50 hores per a la gestió d'incidents de seguretat o sol·licituds no planificades.

5.2. Perfils professionals mínims requerits

El licitador haurà de disposar i assignar a aquest servei d'un equip de treball que compleixi amb els següents perfils professionals mínims, amb l'objectiu de garantir la correcta execució dels serveis objecte d'aquest plec:

a. Expert en seguretat de la informació:
   - Titulació universitària en enginyeria informàtica, telecomunicacions o similar.
   - Experiència mínima de 5 anys en gestió de la seguretat de la informació.

b. Especialista en Esquema Nacional de Seguretat (ENS) i protecció de dades:
   - Titulació universitària en Dret i inscripció vigent com a advocat/ada en un Col·legi d'Advocats.
   - Coneixements avançats en RGPD i LOPDGDD i Esquema Nacional de Seguretat (ENS).

c. Analista de seguretat:
   - Titulació universitària o de Tècnic Superior en Informàtica, Ciberseguretat o àrees relacionades.
   - Experiència mínima de 3 anys en l'ús d'eines de ciberseguretat, anàlisi de vulnerabilitats i proves d'intrusió.

d. Perit Judicial Informàtic Forense:
   - Titulació universitària o de Tècnic Superior en Informàtica, Ciberseguretat o àrees relacionades.
   - Experiència mínima de 3 anys en tasques de perit informàtic Forense.

5.3. Altres consideracions

5.3.1. Conformitat amb l'Esquema Nacional de Seguretat (ENS)

La empresa adjudicatària haurà d'acreditar la conformitat amb l'Esquema Nacional de Seguretat (ENS) en categoria mitja per a tots els serveis inclosos en aquest plec. A tal efecte, s'haurà d'adjuntar a la memòria tècnica el corresponent certificat emès per l'entitat certificadora en el que s'especifiquin aquests serveis dins del seu abast.

5.3.2. Llicències de programari

L'oferta presentada ha d'incloure les llicències necessàries per a una plataforma en línia unificada que permeti cobrir tots els requisits indicats en els serveis detallats a l'apartat 'Altres serveis'.

5.3.3. Lloc de prestació del servei

Aquest servei es prestarà combinant tasques presencials i remotes (no presencials). Les tasques presencials es realitzaran a:

- La seu de l'ARC, a l'Avinguda de la zona Franca, 107- 08038 Barcelona
- Al CPD actual ubicat al Carrer Doctor Roux, 80 -08036 Barcelona

Cal dir que l'ARC està en ple procés de transformació al Model Corporatiu de la Generalitat i està previst que, entre d'altres mesures, al llarg del 2025 o principis del 2026 l'actual CPD ubicat al C/Doctor Roux 80 desaparegui i es mogui al núvol en un entorn Corporatiu.

El prestatari estarà obligat a utilitzar els seus propis equips informàtics d'usuari: PC, ordinador portàtil o qualsevol altre dispositiu d'informàtica mòbil que consideri necessari. En cap cas l'ARC proveirà dels dispositius informàtics ni telefònics al proveïdor.

5.3.4. Horari

Les tasques establertes en aquest servei, es realitzaran dintre de l'horari laboral de l'ARC llevat que les intervencions planificades interfereixin en el bon funcionament dels sistemes informàtics. Si és aquest el cas, es podrà planificar les intervencions fora de l'horari laboral sempre amb la conformitat prèvia de l'ARC.

En cas d'incident de seguretat, caldrà proporcionar un suport continu en les operacions de seguretat, amb actuacions fora de l'horari laboral, si és necessari per mitigar l'incident.

Totes les actuacions fora de l'horari laboral, en el cas que siguin necessàries, estaran incloses dins l'abast de la proposta.

5.3.5. Certificacions

En la presentació de l'oferta s'hauran d'aportar còpies de les certificacions, títols i col·legiació del personal assignat al servei. Els certificats aportats hauran d'estar vigents a la data de presentació de les ofertes.

6.- PROPOSTA TÈCNICA

Els licitadors poden adjuntar a la seva oferta tota la informació complementària que considerin d'interès. Tot i això, haurà de presentar uns continguts mínims i estar obligatòriament estructurada de la forma que s'indica als annexos adjunts:

- Annex 1: model de proposta per a la documentació relativa als criteris de judici de valor.
- Annex 2: model de proposta per a la documentació relativa als criteris ponderables de forma automàtica.

7.- CONFIDENCIALITAT

Tota la informació facilitada per l'ARC que l'empresa contractada hagi d'utilitzar per motius professionals, es considerarà estrictament confidencial i així serà tractada.

8.- PRESSUPOST

El preu s'ha determinat a partir dels preus de mercat del maquinari, programari i suport, objectes del present contracte un cop consultades empreses especialitzades del sector. A partir d'aquest càlcul, determinem que el preu, a tant alçat, d'aquesta licitació serà de 65.000 € + 13.650 € que corresponen al 21% de l'IVA.

9.- LLIURAMENT I PAGAMENT

El pagament es farà mensualment, prèvia presentació de la factura corresponent, contra la certificació acreditativa per part del Cap del Departament de Tecnologies de la Informació de la correcta realització del subministrament i de les tasques efectuades.

El Cap del Departament de
Tecnologies de la Informació

Agència de Residus de Catalunya

ANNEX 1

MODEL DE PROPOSTA PER A LA DOCUMENTACIÓ RELATIVA ALS CRITERIS DE JUDICI DE VALOR PER AL SUBMINISTRAMENT DELS SERVEIS D'OFICINA TÈCNICA DE SEGURETAT PER DONAR SUPORT A L'AGÈNCIA DE RESIDUS DE CATALUNYA (ARC)

PUNTUACIÓ TOTAL: 30 PUNTS

- **Descripció dels serveis oferts en l'apartat "5.1.4 Altres serveis" (puntuació màxima: 15 punts).**
  D'aquesta descripció es valorarà el detall dels serveis oferts per donar resposta als requeriments de l'apartat "5.1.4 Altres serveis", idoneïtat i adequació amb les necessitats de l'ARC, integració amb la resta de serveis de l'Oficina Tècnica de Seguretat i nivell de compliment normatiu. Aquesta descripció no haurà de superar les 6 pàgines en format A4, utilitzant la tipografia Arial 10.

- **Proposta de planificació del servei pel primer any. (puntuació màxima: 8 punts).**
  D'aquesta proposta de planificació es valorarà la seva adequació als requisits tècnics, la idoneïtat i qualitat de les tasques, la capacitat de gestió, execució i seguiment, la innovació i la claredat de la presentació. Aquesta planificació s'ha de presentar en una única pàgina en format A4.

- **Model de relació i gestió del projecte (puntuació màxima: 7 punts).**
  En aquest model de relació i gestió del projecte, es valorarà la claredat, la facilitat de seguiment, la facilitat de comunicació, la claredat en la definició de responsabilitats, l'adaptabilitat a canvis, i la capacitat per a resoldre problemes i complir els objectius definits. Aquesta descripció no haurà de superar les 10 pàgines en format A4, utilitzant la tipografia Arial 10.

ANNEX 2

MODEL DE PROPOSTA PER A LA DOCUMENTACIÓ RELATIVA ALS CRITERIS PONDERABLES AUTOMÀTICAMENT DEL LOT 1 PER AL SUBMINISTRAMENT DELS SERVEIS D'OFICINA TÈCNICA DE SEGURETAT PER DONAR SUPORT A L'AGÈNCIA DE RESIDUS DE CATALUNYA (ARC)

PUNTUACIÓ TOTAL: 70 PUNTS

- **Oferta econòmica (puntuació màxima: 40 punts)**

La fórmula de càlcul d'aquest criteri serà la següent:

$$P_v = \left[1 - \left(\frac{O_v - Om}{IL}\right) \times \left(\frac{1}{VP}\right)\right] \times P$$

Pv = Puntuació de l'oferta a valorar P = Punts criteri econòmic (30 punts)

Om = Oferta millor Ov = Oferta a valorar

IL = Import de licitació VP = Valor de ponderació

Ateses les característiques crítiques d'aquest projecte, el VP serà igual a 4

- **Acreditar la conformitat amb l'Esquema Nacional de Seguretat (ENS) en categoria alta (puntuació màxima: 10 punts)**

Acreditar la conformitat amb l'Esquema Nacional de Seguretat (ENS) en categoria alta per a tots els serveis inclosos en aquest plec. (10 punts)

- **Disposar de certificacions tècniques (puntuació màxima: 20 punts)**

Es concediran punts addicionals per les certificacions tècniques reconegudes en l'àmbit de la ciberseguretat, que demostrin un alt nivell de coneixements i habilitats en les àrees pertinents dels perfils professionals assignats a aquest servei.

- 1 perfil amb títol de Màster Universitari Oficial en Ciberseguretat. (5 punts).
- 1 perfil amb el certificat de Perit Judicial Informàtic Forense col·legiat (5 punts).
- 1 perfil amb el certificat Certified Ethical Hacker (CEH) (5 punts).
- 1 perfil amb el certificat Offensive Security Certified Professional (OSCP) (5 punts).

No s'atorgaran punts per presentar més d'un perfil amb la mateixa certificació.