

**Plec de Prescripcions Tècniques per a la contractació
mitjançant procediment obert subjecte a regulació
harmonitzada els serveis de:**

Oficina de Ciberseguretat ATM

(Exp. C-33/2023)

Agost 2024

ÍNDEX

1.	Context	3
2.	Fites i objectius	4
3.	Objecte del contracte	5
4.	Activitats i funcions de l'empresa adjudicatària	5
4.1.	Analista tècnic de ciberseguretat	6
4.2.	Analista tècnic de dades	6
4.3.	Gestor documental de ciberseguretat.	7
4.4.	Coordinador de l'Oficina de Ciberseguretat.	7
5.	Finalitats i objectius a assolir	8
6.	Requeriments tècnics generals obligatoris de la prestació	8
7.	Formes de seguiment i control de l'execució de les condicions.	10
8.	Calendari de treball i durada del Contracte	11
9.	Condicions generals d'execució i ciberseguretat.....	11
9.1.	Principis bàsics	11
9.2.	Marc de compliment normatiu	12
9.2.1.	Dades de caràcter personal.	12
9.2.2.	Esquema Nacional de Seguretat (ENS).....	12
9.3.	Seguiment	13
10.	Documentació tècnica que han d'aportar les empreses licitadores	13

Número d'expedient: C-33/2023

El contingut d'aquestes prescripcions tècniques deriva del projecte *Implantació del projecte T-mobilitat (reforç de ciberseguretat)* que es troba dins el component 6 inversió 4: “*Digitalització dels serveis administratius que es presten per part de les Comunitats Autònomes i les ciutats de Ceuta i Melilla, en relació amb el transport de mercaderies i de viatgers per carretera o ferrocarril de la seva competència. En aquest àmbit s'inclouran els projectes digitals necessaris per a poder oferir un servei de transport a la demanda, en l'àmbit competencial de les Comunitats Autònomes i les ciutats de Ceuta i Melilla*” (dins de la submesura 15 de la inversió 4 del PRTR) i Reglament (UE) 2021/241 del Parlament Europeu i del Consell de 12 de febrer de 2021, pel qual s'estableix el mecanisme de Recuperació i Resiliència, en el marc del Pla de Recuperació, Transformació i Resiliència – Finançat per la UE - NextGenerationEU.

Aquest projecte es va aprovar en el marc del Pla de Recuperació, Transformació i Resiliència, que inclou les actuacions en el marc del component 6, derivades de l'Acord de la Conferència Nacional de Transports de 20 de juny de 2022, per la qual es modifica la resolució de 24 de novembre de 2021, la qual formalitzava els compromisos financers amb la Comunitat Autònoma de Catalunya per a l'exercici 2021 per al finançament d'actuacions en el marc del component 6, derivats de l'acord de la conferència nacional de transports de 5 de novembre de 2021 pel qual es fixen els criteris de distribució territorial de crèdits pressupostaris dels exercicis 2021 i 2022, així com la distribució corresponent a l'exercici de 2021, per a la finançament d'actuacions d'inversió al marc dels components 1 “pla de xoc de mobilitat sostenible, segura i connectada en entorns urbans i metropolitans” i 6 “mobilitat sostenible, segura i connectada” del pla de recuperació, transformació i resiliència.

Entre les actuacions objecte de finançament contingudes a la resolució de 24 de novembre de 2021 de la secretaria d'Estat de Transports, Mobilitat i Agenda Urbana es troba la de implementació de millores de ciberseguretat en el projecte T-mobilitat, que està inclosa en el component 6 “mobilitat sostenible, segura i connectada”.

Dins de l'abast d'aquest projecte es troba la contractació relativa als serveis de la “Oficina de Ciberseguretat ATM” objecte de licitació d'acord amb allò previst als presents plecs.

Amb la mera presentació de la seva oferta, l'empresa licitadora accepta les prescripcions tècniques establertes en aquest plec.

Qualsevol proposta que no s'ajusti als requeriments mínims establerts en aquest plec quedarà automàticament exclosa de la licitació.

1. Context

L'Autoritat del Transport Metropolità de l'àrea de Barcelona (en endavant ATM) és un consorci interadministratiu de caràcter voluntari, creat el 1997. Actualment, les administracions consorciades són la Generalitat de Catalunya (51%) i administracions locals (49%), compostes per l'Ajuntament de Barcelona, l'Àrea Metropolitana de Barcelona (anteriorment denominada Entitat Metropolitana del Transport) i l'Associació de Municipis per a la Mobilitat i el Transport Urbà (AMTU), al qual es poden adherir totes les administracions titulars de serveis públics de transport col·lectiu, que pertanyin a l'àmbit format per les comarques de l'Alt Penedès, l'Anoia, el Bages, el Baix Llobregat, el Barcelonès, el Berguedà, el Garraf, el Maresme, Osona, el Vallès Occidental i el Vallès Oriental. A més, l'Administració General de l'Estat és present en els òrgans de govern de l'ATM en qualitat d'observador.

L'Àrea de Sistemes i Innovació té encomanades, entre d'altres, la gestió de les polítiques de seguretat informàtica i de protecció de dades, la dels sistemes de seguretat en xarxa i la dels sistemes corporatius d'autenticació d'usuaris. Aquesta Àrea administra una infraestructura de comunicacions i servidors que proporciona el suport sobre el qual s'implementen les aplicacions corporatives, es distribueix la informació dels seus serveis i es presten els serveis telemàtics als ciutadans. En consonància amb el principi bàsic de "Línies de defensa" establert en el Reial decret 311/2022 del 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), per assegurar aquestes comunicacions, cal orientar l'estratègia de seguretat cap a una solució d'arquitectura multicapa, consistent a introduir múltiples capes de seguretat que permetin reduir la probabilitat que els sistemes d'informació es vegin compromesos i minimitzar l'impacte si la situació de risc arriba a materialitzar-se.

Tenint en compte l'evolució i expansió dels ciberatacs durant aquests últims anys, el reforç de la protecció de la ciberseguretat es considera necessari per mitigar en tot el possible els efectes d'aquests atacs.

L'augment d'eines de ciberseguretat i la seva explotació, el control de les dades de les organitzacions, així com la necessitat d'adaptar-se a les diferents normatives com l'ENS o a estàndards com ISO, implica a l'ATM la necessitat de disposar d'una Oficina de Ciberseguretat que en coordinació amb el CISO, pugui establir el marc ideal en la gestió de la ciberseguretat i la protecció de les dades.

En el present Plec de Prescripcions Tècniques es descriuen les necessitats al respecte.

2. Fites i objectius

Que la Unió Europea (UE) va crear els Fons Next Generation EU (d'ara endavant, NGEU) per ajudar a mitigar l'impacte econòmic i social de la pandèmia de la COVID-19 i fer que les economies i societats europees fossin més sostenibles i resilients, aprovats mitjançant el Reglament (UE) 2021/241 del Parlament Europeu i del Consell de 12 de febrer de 2021 pel qual s'estableix el Mecanisme de Recuperació i Resiliència (d'ara endavant, MRR).

Que un dels objectius de la Component 6 "mobilitat sostenible, segura i connectada" del MRR és la "Digitalització dels serveis administratius que es presten per part de les comunitats autònomes i les ciutats de Ceuta i Melilla, en relació amb el transport de mercaderies i de viatgers per carretera o ferrocarril de la seva competència. En aquest àmbit s'inclouran els projectes digitals necessaris per poder oferir un servei de transport a la demanda, a l'àmbit competencial de les Comunitats Autònomes i les ciutats de Ceuta i Melilla (dins de la submesura 15 de la inversió 4 del PRTR".

S'estableixen les fites i objectius següents associades a l'execució del contracte:

Fita 1: Es preveu la finalització del projecte abans del 20 de juny del 2026.

L'adjudicatari haurà de facilitar, en temps i forma, la informació que li sigui requerida per acreditar el compliment de les fites i objectius fixats. La manca de lliurament d'aquesta informació o el seu lliurament incomplet fora de termini o sense respectar les especificacions d'aquest Plec i resta de prescripcions tècniques del contracte, podrà ser considerada causa d'incompliment.

En cas d'incompliment per causa imputable a l'Adjudicatari de les fites i objectius establerts, donarà lloc a la imposició de les penalitzacions previstes en la clàusula 22 del Plec de Clàusules Administratives.

L'incompliment de les fites i objectius establerts, atès el seu caràcter de condició essencial d'execució és causa de resolució del contracte d'acord amb la clàusula 39 del Plec.

Pel que fa als mecanismes per al control de les fites i els objectius, l'empresa adjudicatària haurà de col·laborar en tot allò que li sigui requerit per a la verificació, seguiment i compliment de les obligacions derivades de la normativa interna i europea fixades pel Mecanisme de Recuperació i Resiliència de la UE que s'estableixin.

3. Objecte del contracte

L'objecte d'aquest contracte és la implementació d'una Oficina de Ciberseguretat de l'ATM, que estarà en dependència del CISO i integrada en l'Àrea de Sistemes i Innovació.

Tenint en compte l'evolució i expansió dels ciberatacs durant aquests últims anys, el reforç de la protecció de la ciberseguretat es considera necessari per mitigar en tot el possible els efectes d'aquests atacs.

Amb aquest objectiu, l'ATM requereix disposar d'una Oficina de Ciberseguretat que en coordinació amb el CISO, pugui establir el marc ideal en la gestió de la ciberseguretat i la protecció de les dades, que podrà donar resposta i coordinar la necessitat d'augmentar les eines de ciberseguretat i la seva explotació, el control de les dades de les organitzacions, així com la necessitat d'adaptar-se a les diferents normatives com l'ENS o a estàndards com ISO.

Les organitzacions s'han hagut d'adaptar a les normatives vigents, GDPR, ENS. En paral·lel, la complexitat dels òrgans de govern de la ciberseguretat en les organitzacions també s'ha hagut d'adaptar.

Al respecte, l'ATM disposa de la figura d'un servei de CISO, però ara es creu necessari augmentar la capacitat de la gestió de la ciberseguretat amb la configuració de l'Oficina de Ciberseguretat ATM, que en coordinació amb el CISO i integrada en l'Àrea de Sistemes i Innovació, pugui establir el marc ideal en la gestió de la ciberseguretat i la protecció de les dades.

Per aquestes raons es considera necessari la contractació de la integració de diferents rols en l'Oficina de Ciberseguretat de l'ATM: un rol d'analista tècnic de ciberseguretat, un rol d'analista tècnic de dades, un rol de gestor documental de ciberseguretat i un rol de coordinador de l'Oficina de Ciberseguretat.

4. Activitats i funcions de l'empresa adjudicatària

La prestació regulada en aquest plec ha d'ajustar-se, als requisits tècnics especificats en aquest Plec, sens perjudici dels paràmetres que s'han de valorar mitjançant els criteris d'adjudicació establerts.

L'empresa contractista ha de disposar dels suficients mitjans tècnics, materials qualitatius i personals per a desenvolupar les tasques objecte del corresponent contracte.

La prestació del servei haurà de complir amb els paràmetres de qualitat i seguretat establerts per l'ATM, la legislació vigent i les principals normes i bones pràctiques aplicables a les tecnologies de la informació i la comunicació per a garantir la confidencialitat, disponibilitat i integritat de la informació a la que pugui tenir accés l'adjudicatari en virtut del contracte.

Durant la prestació del servei, l'adjudicatari, conjuntament amb l'ATM, definiran les mesures tècniques de seguretat més apropiades per al servei d'acord amb els anàlisi de riscos que es portin a terme a tal efecte en cas que així es requereixi.

L'oferta que presenti l'empresa licitadora haurà d'abastar la totalitat de la prestació de serveis i realització de les tasques especificades en el present plec i en el Plec de Clàusules Administratives Particulars, essent totes elles obligatòries per a l'admissió de les propostes.

A continuació es descriuen les tasques a realitzar per part de cadascun dels perfils que compondran l'oficina de Ciberseguretat:

4.1. Analista tècnic de ciberseguretat

Aquest perfil ha de dur a terme el control de les eines de ciberseguretat de l'ATM i suport en la validació del marc normatiu.

Les activitats i funcions a realitzar per aquest perfil, a títol enunciatiu que no limitatiu, són els següents:

- Assegurar la disponibilitat en estat òptim i abast de les eines
- Assegurar la monitorització, tractament i escalat de les alertes
- Realitzar informes i quadres de comandament del estat i activitat de les eines
- Proposar i participar en la incorporació de noves eines
- Donar suport a les altres àrees de l'oficina de ciberseguretat per validar els procediments operatius de l'explotació dels sistemes, així com de les evidències aportades pels administradors de sistemes i serveis, en el marc del compliment normatiu.

4.2. Analista tècnic de dades

Aquest perfil ha de dur a terme l'explotació de la informació continguda en diferents repositoris i bases de dades de l'ATM i de la seva protecció. Treballarà en col·laboració amb el responsable de dades de l'Àrea de Sistemes i Innovació de l'ATM.

Les activitats i funcions a realitzar per aquest perfil, a títol enunciatiu que no limitatiu, són els següents:

- Detecció de dades sensibles
- Protecció de les dades
- Creació de consultes en les diferents bases de dades
- Creació d'informes d'ús i rendiment de les bases de dades
- Explotació de les eines de BI (Business Intelligence)
- Revisió de regulacions i afectacions a ATM a nivell protecció de les dades
- Disseny de la monitorització i auditoria de dades
- Documentació de l'estructura de les bases de dades
- Gestió de tasques d'informàtica forense

L'analista tècnic de dades haurà de:

- Mantenir la informació del mapa de dades dels sistemes d'informació de l'ATM.
- Col·laborar amb la definició de directrius i procediments per al compliment de les polítiques dels sistemes d'informació de l'ATM, realitzar la seva implementació, i monitoritzar-ne l'aplicació.

4.3. Gestor documental de ciberseguretat.

Les activitats i funcions a realitzar per aquest perfil, a títol enunciatiu que no limitatiu, són els següents:

- Validació i manteniment de la política de gestió documental de ciberseguretat de l'ATM.
- Modificació, actualització i manteniment del marc documental basat en la política de seguretat de la informació.
- Establiment de rols i responsabilitats per a la gestió de la documentació de seguretat.
- Identificació i classificació de la informació en funció de la seva importància, sensibilitat o criticitat.
- Definició del cicle de vida de la informació.
- Implementació de controls de versions que garanteixi la correcta actualització i vigència dels documents i la informació que aquests contenen.
- Establiment dels processos d'aprovació i accés als documents i la informació continguda.
- Validació i manteniment del contingut del Sistema de Gestió de la Seguretat de la Informació (SGSI). El fons documental estarà principalment en un repositori organitzat segons els capítols d'un SGSI basat en l'estàndard ISO/IEC 27001.

4.4. Coordinador de l'Oficina de Ciberseguretat.

Aquest perfil serà el responsable de la coordinació de l'Oficina de Ciberseguretat de l'ATM depenent del CISO.

Les activitats i funcions a realitzar per aquest perfil, a títol enunciatiu que no limitatiu, són els següents:

- Gestionar la governança del marc normatiu (polítiques de seguretat, normes de seguretat, procediments de seguretat y altres de nivells jeràrquics inferiors), coordinació a nivell normatiu dels diferents departaments que conformen l'ATM o que tenen relació directa amb aquest, així com la gestió i alineament del marc normatiu dels proveïdors que subministren serveis i recursos tecnològics a l'ATM.
- Coordinar les accions d'adequació normativa anteriorment descrites amb l'àrea legal de l'ATM (Àrea d'Assessoria Jurídica i Contractació) i la figura del Delegat de Protecció de Dades (DPD) de l'ATM.

- Coordinació i seguiment dels projectes de ciberseguretat de l'ATM, així com de l'operativa en matèria de ciberseguretat.
- Responsable dels informes de seguiment mensual de l'Oficina de Ciberseguretat o altres informes que se li requereixin.

A banda de les tasques descrites en aquesta clàusula, l'adjudicatari durant l'execució del contracte es responsabilitzarà de les tasques de gestió, millores, ajustos i altres aspectes de gestió de la prestació que puguin sorgir.

Els diferents perfils que componen l'Oficina de Ciberseguretat de l'ATM hauran de vetllar per la col·laboració amb aquells actors d'activitats on es requereixi la participació de l'Oficina.

Durant l'execució del contracte, l'adjudicatari haurà de facilitar a la direcció de la contractació qualsevol informació sol·licitada amb un termini màxim de lliurament de 5 dies hàbils.

5. Finalitats i objectius a assolir

La finalitat i objectiu que s'ha d'assolir mitjançant la realització d'aquest contracte és disposar d'una Oficina de Ciberseguretat que en coordinació amb el CISO, pugui establir el marc ideal en la gestió de la ciberseguretat i la protecció de les dades, que podrà donar resposta i coordinar la necessitat d'augmentar les eines de ciberseguretat i la seva explotació, el control de les dades de les organitzacions, així com la necessitat d'adaptar-se a les diferents normatives com l'ENS o a estàndards com ISO.

6. Requeriments tècnics generals obligatoris de la prestació

L'adjudicatari disposarà dels suficients mitjans tècnics, materials qualitatius i personals per desenvolupar les tasques objecte d'aquest contracte.

La prestació regulada en el present plec haurà d'ajustar-se, almenys, als següents requisits tècnics, sens perjudici dels paràmetres a valorar mitjançant els criteris d'adjudicació establerts.

L'adjudicatari haurà de posar a disposició de l'ATM durant el termini d'execució del contracte perfils adients suficientment qualificats, amb la titulació corresponent, formació i experiència especialitzada en les matèries que són objecte del contracte amb els coneixements necessaris per al seu correcte desenvolupament, amb els requisits mínims que s'indiquen a continuació.

A continuació s'identifiquen i es descriuen els diferents perfils a proporcionar per l'adjudicatari, la responsabilitat i el percentatge d'hores de dedicació:

Perfil	Responsabilitat	Dedicació
Analista tècnic de ciberseguretat	Tasques especificades a l'apartat 4.1	100%
Analista tècnic de dades	Tasques especificades a l'apartat 4.2	100%

Gestor documental de ciberseguretat	Tasques especificades a l'apartat 4.3	50%
Coordinador de l'Oficina de Ciberseguretat	Tasques especificades a l'apartat 4.4	75%

L'experiència professional, titulació i coneixements mínims que s'exigeix per aquest perfil són els següents:

Perfil	Titulació/ Experiència/Coneixements
Analista tècnic de ciberseguretat	Titulació: Nivell grau en enginyeria informàtica o telecomunicacions (o equivalent) Experiència: Haver participat en un <u>mínim de 2 projectes</u> durant els darrers 2 anys fent tasques de tècnic informàtic en tasques d'explotació d'eines de ciberseguretat. Coneixements: Es valoraran altres titulacions equivalents i certificacions al sector de la ciberseguretat.
Analista tècnic de dades	Titulació: Nivell grau en enginyeria informàtica i/o telecomunicacions (o equivalent) Experiència: Haver participat en un <u>mínim de 2 projectes</u> durant els darrers 2 anys en gestió de dades. Coneixements: Es valorarà coneixement en consultes en bases de dades (SQL), eines de BI i informes, monitorització i auditoria (Audit Vault – Oracle), així com altres titulacions, certificacions i experiència en l'àmbit de l'explotació de les dades i de la ciberseguretat.
Gestor documental de ciberseguretat	Titulació: Nivell grau universitari Experiència: Haver participat en un <u>mínim de 2 projectes</u> durant els darrers 2 anys en gestió documental. Coneixements: Es valorarà coneixement en estàndards per a la gestió documental com UNE-ISO 30301 i UNE-ISO 27001, o equivalents.
Coordinador de l'Oficina de Ciberseguretat	Titulació: Nivell grau en enginyeria informàtica o telecomunicacions (o equivalent) Experiència: Haver participat en un <u>mínim de 3 projectes</u> durant els darrers de 5 anys en l'àmbit de la gestió de la ciberseguretat, adequació a marcs normatius com RGPD, ENS, PCI,... implementació d'estàndards ISO, NIST,... Coneixements: Es valorarà titulacions, certificacions i experiència en l'àmbit de la ciberseguretat i de l'adequació a normatives a l'Administració Pública.

L'adjudicatari haurà de garantir la continuïtat de la prestació del servei per part de l'equip durant tot el termini d'execució dels treballs, preveient absències per causes planificades o sobrevingudes. Qualsevol canvi haurà d'ésser autoritzat prèviament per l'ATM. Els possibles canvis o modificacions hauran de ser comunicats per escrit a l'ATM amb la deguda antelació i acceptats per aquesta. En aquest supòsit l'adjudicatari haurà de proposar una/es persona/es amb la formació i experiència mínimes requerides en la licitació, i en el seu cas, tenint en compte les característiques de les persones valorat en la licitació, d'acord la seva oferta.

A més, en cas de substitució s'exigirà el següent:

- Un període de formació, a càrrec de l'adjudicatari, pel nou membre que s'incorpori a l'execució del contracte.
- Un període de coexistència, d'un mínim de 15 dies, entre la persona que causa baixa i la persona que s'incorpora.

L'ATM es reserva la facultat de requerir a l'adjudicatari la substitució qualsevol perfil de l'Oficina de Ciberseguretat per tal d'assolir un compliment òptim del contracte.

En aquest ordre de coses, es fa constar que l'ATM queda desvinculada, a tots els efectes, de qualsevol relació laboral amb el personal de l'entitat adjudicatària, atès que es tracta d'un contracte de suport i assistència que ha de ser considerat com a tal en el seu conjunt.

L'empresa contractista està obligada, pel que fa a aquestes persones, al compliment de les disposicions vigents en matèria laboral, de seguretat social i de seguretat i salut en el treball que li siguin d'aplicació.

L'execució del contracte s'interpreta com la prestació d'un servei i el contractista haurà de garantir la continuïtat del mateix. Es durà a terme a les dependències, calendari laboral i horari de l'ATM i es coordinarà amb l'empresa adjudicatària totes les qüestions corresponents a absències, períodes vacacionals, etc.. Es tindrà la possibilitat d'executar les jornades laborals de forma presencial i teletreball, segons requereixi l'ATM.

L'ATM proporcionarà als components de l'Oficina de Ciberseguretat les eines i els equips informàtics necessaris per la realització del treball. Altrament, per a la resta de perfils els adjudicataris hauran d'aportar els equips informàtics necessaris per a la prestació del servei. Els components de l'Oficina de Ciberseguretat disposarà de telèfon mòbil de contacte. L'ATM no proporcionarà el telèfon mòbil ni el servei de telefonia ni dades associades al citat dispositiu. Tampoc assumirà cap despesa de connectivitat en el marc de treball fora de les oficines de l'ATM en termes amplis dins la prestació del servei contractual de referència.

7. Formes de seguiment i control de l'execució de les condicions.

L'òrgan de contractació designarà una persona que assumirà el control i la coordinació de l'execució contractual amb l'empresa adjudicatària per tal de tractar directament les qüestions relacionades amb el desenvolupament normal de les tasques indicades en aquest plec.

L'adjudicatari ha de designar una persona responsable a qui encarregar la gestió de l'execució del contracte i que haurà de garantir la qualitat de la prestació objecte d'aquest plec, tractant directament les qüestions relacionades amb el desenvolupament normal de les tasques indicades en aquest plec amb la persona interlocutora designada per l'òrgan de contractació.

8. Calendari de treball i durada del Contracte

S'estableix una durada del present contracte dels mesos corresponents entre la data d'inici del contracte i la data de finalització d'aquest, fixada el 20 de juny de 2026, per a la prestació dels serveis objecte d'aquest plec.

Dins dels 10 dies següents a la data d'inici de la prestació de l'objecte del contracte, l'empresa contractista haurà de lliurar al responsable del contracte el programa de treball per a la seva acceptació. La direcció del contracte resoldrà sobre el programa de treball dins d'un termini de 5 dies comptats a partir de la data de lliurament, entenent-se que la resolució podrà introduir modificacions, sempre que no contravinguin les condicions del contracte.

9. Condicions generals d'execució i ciberseguretat

9.1. Principis bàsics

- **Deure de confidencialitat.** El personal de l'empresa adjudicatària ha de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat té caràcter indefinit i subsistirà inclús després d'haver cessat la seva relació laboral amb l'ATM. L'empresa adjudicatària ha de comunicar aquesta obligació de confidencialitat al seu personal i ha de controlar el seu compliment. L'empresa adjudicatària ha de posar en coneixement de l'ATM, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de la informació. Aquest deure s'estén als empleats d'altres empreses, que a petició de l'adjudicatari, participin a la prestació dels serveis recollits en aquest plec.

- **Propietat intel·lectual:** tota la documentació que es generi durant la prestació dels serveis de suport és propietat exclusiva de l'ATM.

Tota la documentació generada en la present contractació serà propietat de l'ATM i no se'n podrà fer cap ús per part de l'Adjudicatari, així com tots els desenvolupaments realitzats dins de la present licitació.

- **Criteris d'accessibilitat universal:** l'empresa adjudicatària es responsabilitzarà de complir amb els criteris d'accessibilitat universal, tal com són definits aquests termes al text refós de la Llei General de drets de les persones amb discapacitat i d'inclusió social, aprovat mitjançant Reial Decret Legislatiu 1/2013, de 29 de novembre.

Els mitjans de comunicació, el disseny dels elements instrumentals i la implantació dels tràmits procedimentals emprats per l'empresa contractista en l'execució del contracte hauran de realitzar-se tenint en compte els criteris d'accessibilitat universal i de disseny per a tothom.

- **Criteris de sostenibilitat i protecció al medi ambient:** l'empresa adjudicatària es responsabilitzarà de complir els criteris de sostenibilitat i protecció del medi ambient, d'acord amb les definicions i principis regulats als articles 3 i 4, respectivament, del *Reial Decret Legislatiu 1/2016, de 16 de desembre, pel qual s'aprova el text refós de la Llei de prevenció i control integrats de la contaminació.*

Sempre que sigui possible, l'empresa contractista haurà de fer una elecció intel·ligent de materials (ús de materials adequats per al medi ambient, evitant els que no ho siguin), equips d'eficiència energètica (reduir el cost energètic i la petjada de carboni col·lectiu), final de la vida útil i reutilització, etc.

9.2. Marc de compliment normatiu

L'actual marc normatiu per a les entitats públiques de Catalunya, està establert, principalment, a la Política de Ciberseguretat de la Generalitat de Catalunya de setembre del 2021. Aquesta política recull directives i reglaments del Parlament i Consell Europeu, reials decrets de l'estat espanyol, així com instruccions de la Generalitat de Catalunya. Aquest marc de compliment normatiu en temes de ciberseguretat i protecció de dades, abasta a les entitats públiques de la Generalitat de Catalunya i a tots aquells que participen en la prestació dels seus serveis.

9.2.1. Dades de caràcter personal.

L'adjudicatari tractarà les dades de caràcter personal a què accedeixi com a conseqüència de l'execució d'aquest contracte de conformitat amb allò establert a la normativa vigent en la matèria.

L'empresa adjudicatària es responsabilitzarà de l'ús adequat de la informació que es pugui obtenir per tal de protegir les dades personals, al llarg de tota la fase de realització de l'objecte del contracte i també una vegada finalitzada sobre la base de les normatives internacionals sobre això i de compliment obligat, entre ells i expressament, el Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, sobre la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació de les dades esmentades, així com qualsevol altra normativa nacional i de la Unió Europea que sigui aplicable en matèria de protecció de dades i en relació amb les dades personals a què té accés durant la vigència d'aquest contracte.

L'incompliment d'aquestes obligacions constitueix la infracció tipificada a la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia de drets digitals, sens perjudici de les responsabilitats exigides davant la jurisdicció ordinària.

L'Adjudicatari amb relació a aquelles dades que per la Llei Orgànica de Protecció de Dades i Garantia dels Drets Digitals (LOPDGDD) sigui necessari, en la solució proposada ho ha complir, p. ex. ubicar les dades en una base de dades física diferent, xifrar les dades, control d'accés, etc.

L'Adjudicatari es compromet a complir, amb relació a les dades tractades en l'execució del present contracte:

- La Llei Orgànica de Protecció de Dades i Garantia dels Drets Digitals (LOPDGDD).
- les bones pràctiques per a la gestió de la seguretat de la informació

9.2.2. Esquema Nacional de Seguretat (ENS)

L'article 2 del vigent Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, disposa que els plecs de prescripcions administratives o

tècniques dels contractes que celebrin les entitats del sector públic incloses en l'àmbit d'aplicació del reial decret del ENS contemplaran tots aquells requisits necessaris per a assegurar la conformitat amb el mateix dels sistemes d'informació en els quals se sustentin els serveis prestats pels contractistes, com ara la presentació de les corresponents Declaracions o Certificacions de Conformitat amb el ENS. Aquesta cautela s'estendrà també a la cadena de serveis d'aquests contractistes, en la mesura que sigui necessari i d'acord amb els resultats de la corresponent anàlisi de riscos.

L'ATM, considera necessari que els proveïdors que vagin a concórrer a aquesta licitació hauran d'estar en condicions d'exhibir una Declaració de Conformitat amb l'ENS. Així doncs, sobre la base de l'anterior, i a l'anàlisi dels riscos als quals estan exposats els serveis objecte de la licitació, l'ATM estableix com a necessari que les entitats licitadores hauran d'estar en condicions d'exhibir la corresponent Declaració de Conformitat amb l'Esquema Nacional de Seguretat, així com mantenir la conformitat en vigor durant la vigència del contracte. Aquesta declaració de conformitat amb l'ENS ha d'abastar l'àmbit objecte de la contractació.

Per altra banda, s'ha establert com a criteri objectiu de valoració de les ofertes el disposar per part dels licitadors d'un nivell superior de conformitat a l'Esquema Nacional de Seguretat, de manera que el licitador adjudicatari haurà de mantenir el nivell declarat durant tot el termini d'execució del contracte.

En el cas que l'adjudicatari no pogués mantenir la conformitat amb l'ENS durant la vigència del contracte -per impossibilitat de mantenir la Declaració de Conformitat o pèrdua, retirada o suspensió de la Certificació de Conformitat-, haurà de comunicar aquesta circumstància, de manera immediata i sense dilació indeguda, a l'ATM, qui considerarà l'impacte d'aquesta circumstància en la prestació objecte del contracte.

S'estableix un mecanisme provisional d'acreditació de compliment amb l'ENS, que consisteix amb la possibilitat dels proveïdors de presentar informes d'auditoria, declaracions d'aplicabilitat o processos de certificació en curs, l'acceptació d'aquests documents dependrà de la validació per part de l'ATM.

Es valorarà un major nivell del compliment de l'ENS per sobre del mínim requerit.

Els requeriments d'aquest marc de compliment normatiu, no exclouen d'altres requeriments de ciberseguretat que puguin estar inclosos en aquest plec.

9.3. Seguiment

L'adjudicatari assignarà un responsable de seguretat i protecció de dades per tractar els temes de ciberseguretat. L'adjudicatari lliurarà durant l'execució del contracte un model de seguiment de la ciberseguretat en funció de la fase del projecte.

Aquest responsable podrà coincidir amb el perfil del Coordinador de l'Oficina de Ciberseguretat ofert per l'adjudicatari.

10. Documentació tècnica que han d'aportar les empreses licitadores

Les especificacions tècniques proposades per l'empresa licitadora en la seva oferta esdevindran condicions de compliment obligat al llarg de l'execució del contracte si aquesta esdevé l'adjudicatària.

El licitador haurà de presentar una proposta tècnica d'acord amb el model de l'annex 1 del PCA, que inclourà en tot cas:

- Descripció dels diferents perfils de l'Oficina de Ciberseguretat que posaran a disposició del contracte, que inclogui la titulació, formació, coneixements i experiència de l'equip de treball, que ha de complir amb els requeriments mínims establerts en aquest Plec.
- La proposta tècnica haurà d'incloure una descripció de la metodologia de treball que proposa el licitador per al desenvolupament del servei tenint en compte la sistemàtica que utilitzarà per a dur a terme la prestació amb les especificitats particulars que garanteixin la seva correcta execució i interrelació amb l'ATM.
- Caldrà que s'inclogui la descripció de la metodologia pel que fa al control i seguiment de l'equip, la descripció del control i seguiment del servei així com de les eines de gestió que s'empraran per a la realització dels serveis a contractar.

Carme Fàbregas Casas
Directora de l'Àrea de Sistemes i Innovació

Signat electrònicament