

**Plec de Prescripcions Tècniques per a la contractació
mitjançant procediment obert pels serveis de:**

**ADEQUACIÓ A L'ESQUEMA NACIONAL DE SEGURETAT
(ENS) EN EL MARC DEL PLA DE RECUPERACIÓ,
TRANSFORMACIÓ I RESILIÈNCIA - FINANÇAT PER LA UE -
NEXT GENERATION EU ”¹**

(Exp. C-27/2023)

Octubre 2024

¹ Mecanisme de Recuperació i Resiliència.

Ajudes concedides per al compliment de les CID (Council Implementing Decision, o Decisió d'Execució del Consell) núm. 101 "Suport al programa de transport sostenible i digital: Finalització de les obres", en el marc del component 6, inversió 4: «Programa de suport per a un transport sostenible i digital» dins de la submesura 15: "Projectes per a la digitalització dels serveis de transport de passatgers i mercaderies en l'àmbit autonòmic i local", derivades d'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 2021, per al finançament de les actuacions d'inversió en el marc dels components 1 del Pla de xoc de mobilitat sostenible, segura i connectada en entorns urbans i metropolitans i 6 Mobilitat sostenible, segura i connectada del PRTR, concretament, per als projectes de "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".

ÍNDEX

1.	Context	3
2.	Fites i objectius	5
3.	Objecte del contracte	5
4.	Activitats i funcions de l'empresa adjudicatària	8
4.1.	Desenvolupament de les fases d'adequació	8
4.2.	Documentació a lliurar	10
4.2.1.	Gestió documental	10
4.2.2.	Lliurables	10
5.	Finalitats i objectius a assolir	13
6.	Requeriments tècnics generals obligatoris de la prestació	13
6.1.	Equip de treball	13
7.	Formes de seguiment i control de l'execució de les condicions	15
8.	Calendari de treball i durada del Contracte	15
9.	Condicions generals d'execució i ciberseguretat	16
9.1.	Principis bàsics	16
9.2.	Marc de compliment normatiu	16
9.2.1.	Dades de caràcter personal	17
9.2.2.	Esquema Nacional de Seguretat (ENS)	17
9.2.3.	Seguiment	18
10.	Documentació tècnica que han d'aportar les empreses licitadores	18

Número d'expedient: C-27/2023

1. Context

Mitjançant Resolució de 19 de juliol de 2022 de la Secretaria d'Estat de Transports, Mobilitat i Agenda Urbana, es van formalitzar 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, derivades 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 2021, per al finançament de les actuacions d'inversió en el marc dels components 1 del 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 (d'ara endavant, el **"Acord de la Conferència Nacional de Transports"** i **"PRTR"** respectivament).

Dins de les actuacions objecte de finançament contingudes en la citada resolució, es troba la ciberseguretat del Projecte T-mobilitat Catalunya i Autoritat del Transport Metropolità (d'ara endavant, el **"Projecte"**), amb un import de 2.315.000,00 euros. Està inclosa en el component 6 Mobilitat sostenible, segura i connectada del PRTR.

Per això, i d'acord amb el que es preveu en el Capítol VI de la Llei 40/2015, d'1 d'octubre de règim jurídic del sector públic (d'ara endavant, **"Llei 40/2015"**); els articles 108 a 112 de la Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya (en endavant, **"Llei 26/2010"**); Reial decret llei 36/2020, de 30 de desembre, pel qual s'aproven mesures urgents per a la modernització de l'Administració pública i per a l'execució del Pla de recuperació, transformació i resiliència (d'ara endavant, **"RDL 36/2020"**), i l'article 6 de la Llei 9/2017, de 8 de novembre, de contractes del sector públic (en endavant, **"LCSP"**), el Departament de Territori de la Generalitat de Catalunya (en endavant, la **"DTER"**) i el Consorci de l'Autoritat de Transport Metropolità de Barcelona (en endavant, **"ATM"**) van articular a l'abril de 2024 el Conveni de col·laboració per a la ciberseguretat del Projecte T-Mobilitat, amb càrrec als Fons Europeus del Mecanisme per a la Recuperació i Resiliència (d'ara endavant, el **"Conveni"** i **"MRR"**, respectivament).

L'objecte del citat Conveni és l'establiment d'un marc de col·laboració entre el DTER i la ATM per a dur a terme l'actuació de la ciberseguretat del projecte T-mobilitat Catalunya i Autoritat del Transport Metropolità, dins del marc de les competències que corresponen a aquesta ATM, a càrrec dels fons europeus procedents del MRR.

Aquest projecte té per objecte dur a terme un conjunt d'actuacions que es resumeixen en l'adquisició i l'explotació d'eines de ciberseguretat, el govern de la ciberseguretat i l'adequació a les normatives d'obligat compliment, que comporta la protecció de tots els actius d'informació de la T-mobilitat i dels sistemes de la ATM i, especialment, dels sistemes d'informació.

El repte del projecte T-mobilitat és transformar i modernitzar els sistemes de venda i validació del transport públic amb la finalitat de permetre la implantació del sistema d'integració tarifària en el conjunt del territori de Catalunya perquè l'usuari tingui la possibilitat de fer intercanvis modals independentment de la zona i del mitjà de transport i, al mateix temps, garantir un tracte tarifari homogeni.

A causa de l'evolució i expansió dels atacs durant aquests últims anys, el reforç de la protecció de la ciberseguretat es considera necessari per a mitigar tant com sigui possible, els efectes dels atacs que rebrà.

A causa de l'evolució i expansió dels atacs durant aquests últims anys, el reforç de la protecció de la ciberseguretat es considera necessari per a mitigar tant com sigui possible, els efectes dels atacs que rebrà.

Per a aconseguir-ho, en l'annex I del Conveni es relacionen les actuacions a desenvolupar, així com les metes, objectius i costos de cadascuna.

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.

En aquest context, 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.

La Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics va establir l'Esquema Nacional de Seguretat (ENS) que, aprovat mitjançant Reial decret 3/2010, de 8 de gener, i posteriorment modificat pels Reials decrets 951/2015 i 311/2022, està constituït pels principis bàsics i requisits mínims que permeten una protecció adequada de la informació. El seu abast afecta als sistemes d'informació, les dades, les comunicacions i els serveis electrònics de qualsevol Administració Pública i la seva cadena de subministrament, per a assegurar l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informacions i serveis utilitzats en mitjans electrònics que es gestionin en l'exercici de les seves competències. L'ATM necessita adequar-se a l'Esquema Nacional de Seguretat en compliment de la legislació vigent.

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

Dins de l'abast d'aquest projecte es troba la contractació relativa als serveis per a l'adequació de la ATM a l'Esquema Nacional de Seguretat (ENS) 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

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 prestació de serveis per a l'adequació dels sistemes d'informació de l'ATM a l'Esquema Nacional de Seguretat (ENS), regulat pel Reial decret 311/2022 pel qual es regula l'Esquema Nacional de Seguretat i les Instruccions Tècniques de Seguretat publicades pel Centre Criptològic Nacional, dels sistemes i serveis tecnològics de l'ATM, definint i executant un pla d'adequació, elaborant la documentació necessària per a aquesta adequació.

L'execució d'aquest contracte comportarà la realització dels serveis de consultoria per a la realització d'una anàlisi de l'estat actual de la seguretat, identificar les necessitats utilitzant com a marc el Reial decret 311/2022, per al disseny d'un pla d'adequació específic a l'Esquema Nacional de Seguretat que ens permeti implantar les mesures de seguretat per a aconseguir el compliment de Categoria Mitjana, amb càrrec fons PRTR.

Així mateix, el contracte també inclou el desenvolupament d'un pla d'activitats formatives de conscienciació, sensibilització en ciberseguretat de la informació per al personal de l'ATM.

S'ha estimat que els sistemes de l'ATM tenen un nivell de categoria Mitjà, però la seva classificació definitiva, objecte d'adequació d'aquest contracte, s'obtindrà durant el transcurs de la seva execució

Per a les mesures que requereixin per a la seva implementació la incorporació de serveis addicionals als contractats o productes TIC no inclosos en el present contracte, correran a càrrec de l'ATM. Serà responsabilitat de l'adjudicatari els anàlisis i elaboració de documentació de polítiques i directrius que siguin requerits en l'aplicació del decret.

Si durant la prestació del servei s'identifiquen necessitats de consultoria o elaboració d'algun informe no previstos inicialment en aquest Plec de Prescripcions Tècniques, aquestes hauran de ser assumides per l'adjudicatari.

Així mateix, les prestacions que integren l'objecte del contracte tenen per finalitat el compliment de les CID (Council Implementing Decision, o Decisió d'Execució del Consell) núm. 101 *"Suport al programa de transport sostenible i digital: Finalització de les obres"*, en el marc del 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: *"Projectes per a la digitalització dels serveis de transport de passatgers i mercaderies en l'àmbit autonòmic i local"*, derivades de l'Acord de la Conferència Nacional de Transports, dins de les actuacions objecte de finançament contingudes en la Resolució de 24 de novembre de 2021 de la secretaria d'Estat de Transports, Mobilitat i Agenda Urbana està la ciberseguretat del projecte T-mobilitat Catalunya.

La inversió inclou un conjunt de mesures destinades a 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 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

Número	Mesura	Fita/ Objectiu	Nom	Indicadors qualitatius (per a les fites)	Indicadors quantitatius (per als objectius)		
					Unitat	Referència	Meta
101	C6.I4	Fita	Suport al programa de transport sostenible i digital: Finalització de les obres.	Notificació oficial de la finalització de les obres	-	-	-

Temes		Descripció de la fita/objectiu
Trimestre	Any	
Q2	2026	Projectes per a la digitalització dels serveis de transport de passatgers i mercaderies en l'àmbit autonòmic i local. Finalització de tots els projectes adjudicats en el quart trimestre de 2022 (fita 99) per a promoure el transport sostenible i digital. Les obres estan relacionades amb els àmbits definits en els criteris de selecció del document d'adjudicació del projecte del quart trimestre de 2022..

Mesura: C6.I4 (submesura 15): "Projectes per a la digitalització dels serveis de transport de passatgers i mercaderies en l'àmbit autonòmic i local. Finalització de tots els projectes adjudicats en el quart trimestre de 2022 (fita 99) per a promoure el transport sostenible i digital".

Component: 6 "Mobilitat sostenible, segura i connectada del PRTR".

Inversió: 4 "Programa de suport per a un transport sostenible i digital".

Projecte:

- C6.I4-CCAA: "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".
- Projecte T- Mobilitat Catalunya.

Les actuacions que es duguin a terme a conseqüència del contracte actual respectaran el principi de «no causar un perjudici significatiu al medi ambient» (principi do no significant harm), d'acord amb el que es preveu en el PRTR, així com amb el requerit en la decisió d'execució del Consell relativa a l'aprovació de l'avaluació del PRTR d'Espanya.

Així mateix, el contractista i els subcontractistes estaran obligats a complir:

1. Amb els compromisos en matèria d'etiquetatge verd i digital, així com per l'aplicació del principi de no causar mal significatiu al medi ambient (Do not significant harm, DNSH) establert, si n'hi hagués².
2. L'obligació de, en les comunicacions i la documentació relativa als projectes, subprojectes i actuacions que es desenvolupin en l'execució del Pla, exhibir de manera correcta i destacada l'emblema de la UE amb una declaració de finançament adequat que

² El Reglament del MRR estableix que cap de les mesures d'execució de les reformes i inversions incloses en el PRTR causarà un perjudici significatiu (DNSH) als sis objectius mediambientals definits en el Reglament (UE) núm. 2020/852 del Parlament Europeu i del Consell, de 18 de juny de 2020, relatiu a l'establiment d'un marc per a facilitar les inversions sostenibles i pel qual es modifica el Reglament (UE) 2019/2088, detallats a continuació: Mitigació del canvi climàtic; adaptació al canvi climàtic; ús sostenible i protecció dels recursos hídrics i marins; transició cap a una economia circular; prevenció i control de la contaminació; i protecció i recuperació de la biodiversitat i els ecosistemes.

digui: "Finançat per la UE - NextGenerationEU", juntament amb el logotip oficial del Pla de recuperació, transformació i resiliència (<https://planderecuperacion.gob.es/identidad-visual>). Així mateix, s'incorporarà el logotip oficial dels *Next *Generation Catalunya d'acord amb les seves pautes gràfiques).

4. Activitats i funcions de l'empresa adjudicatària

La prestació regulada en aquest plec ha d'ajustar-se, almenys, 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.

Les funcions que haurà de realitzar l'empresa adjudicatària es desenvoluparan tres fases:

Fase I	Definició del pla d'adequació a l'ENS
Fase II	Execució i seguiment del pla d'adequació
Fase III	Auditoria final de compliment

4.1. Desenvolupament de les fases d'adequació

L'adjudicatari haurà de preparar i/o supervisar, segons el cas, la documentació oportuna que evidenciï el compliment de les tasques de cada fase, amb la finalitat de validar el desenvolupament de les fases que haurà d'assolir el servei.

A títol enunciatiu que no limitatiu, la documentació a preparar/validar en l'execució d'aquest contracte, segons les fases, és la següent:

FASE I: Definició del pla d'adequació a l'ENS

1. IDENTIFICACIÓ I DETERMINACIÓ DE L'ABAST
 - Abast de l'ENS.
 - Mapa de processos.
 - Categorització Sistema.
2. DEFINICIÓ DEL MODEL DE GOVERN
 - Responsables dels Serveis.
 - Responsables de la Informació.
 - Delegat de Protecció de Dades.

- Responsable de la Seguretat de la Informació.
- Responsable del Sistema.
- Comitè de Seguretat de l' ATM.

3. ESTABLIMENT DE LA POLÍTICA DE SEGURETAT

- Proposta de Política de Seguretat al Comitè de Seguretat.
- Preparar recull de les normatives que desenvolupen la política de seguretat que aplicaran a l'ATM
- Suport en l'elaboració de documents tècnics:
 - Mecanismes que cal establir per a la identificació d'anomalies.
 - Sistemes de resolució de les anomalies detectades.
 - Redacció d'Instruccions específiques per als usuaris i responsables dels sistemes d'informació.
 - Redacció de documents tipus per al registre i control de les incidències de seguretat i els procediments associats.
 - Altres documents requerits per assolir el compliment.

4. AVALUACIÓ DEL COMPLIMENT

- Realització de la Declaració d'Aplicabilitat.
- Compliment de les mesures de l'ENS.

5. ELABORACIÓ DEL PLA D'ADEQUACIÓ

- Anàlisi de Riscos.
- Pla de Tractament dels Riscos.
- Disseny del Pla d'Adequació.
- Identificació de recursos necessaris i terminis d'implementació.
- Validació del Pla de Adequació.
- Matriu de correlació dels controls d'aplicabilitat amb RGPD i PCI DSS

FASE II: Execució i seguiment del pla d'adequació

6. EXECUCIÓ I SEGUIMENT DEL PLA D'ADEQUACIÓ

- Implantació de les mesures.
- Avaluació de l'eficàcia de les mesures implantades.

7. PLA DE CONSCIENCIACIÓ EN SEGURETAT

- Elaboració d'un Pla de Conscienciació del Projecte d'Adequació a l'ENS.
- Elaboració d'un Pla de Comunicació i conscienciació en seguretat.
- Elaboració d'un Pla de Formació en seguretat.

FASE III: Auditoria final de compliment

8. AUDITORIA INTERNA DE COMPLIMENT DE L'ENS

- Auditoria interna de compliment
- Elaboració de l'informe pendent del Pla de remediació.
- Presentació d'informe final.

9. PROPOSTA DE MILLORA CONTINUA

- Procediments per a la millora continua (PDCA) enfocat al manteniment i increment del grau de maduresa assolit.

L'adjudicatari haurà d'elaborar els documents necessaris per donar el compliment documental de les diferents fases, amb el format establert per l'ATM.

4.2. Documentació a lliurar

4.2.1. Gestió documental

El contractista haurà de realitzar l'estudi i desenvolupament d'una proposta de sistema de Gestió Documental que doni suport a totes les fases de l'adequació, manteniment i millora contínua del ENS. Aquesta organització de la informació, que l'adjudicatari haurà de desenvolupar en profunditat d'acord amb els requisits establerts en aquesta secció, haurà de comptar amb la seva adequada inclusió i descripció en la política de seguretat.

Malgrat que l'ATM disposa de diferents solucions per l'emmagatzematge de dades, en el marc d'aquesta licitació es requereix als licitadors propostes de solucions de plataformes, de caràcter comercial i lliure, per a la gestió documental.

L'estructuració de la informació proposada ha de ser conforme i donar adequada resposta a tots els punts de verificació descrits en les guies CCN-STIC.

4.2.2. Lliurables

Perquè el servei compleixi els seus objectius es fa necessari l'estricta compliment dels requisits descrits a les Guies CCN-STIC, elaborant i aportant les evidències documentals necessàries per justificar el compliment de l'ENS, realitzant un seguiment continu del grau d'implementació de les mesures de seguretat que apliquin als sistemes.

La llista de lliurables podria veure's alterada en funció del perfil de compliment i de la declaració d'aplicabilitat que s'estableixin per als sistemes de l'ATM:

Compliment dels articles de l'ENS

1. Repositori amb les Guies CCN-STIC utilitzades
2. Registre de legislació i normativa aplicable, incloent-hi les Instruccions Tècniques de Seguretat (ITS)
3. Declaració d'Aplicabilitat
4. Informe de l'Estat de Seguretat (INES)
5. Categorització de sistemes i valoracions d'impacte
6. I aquells que es derivin de les particularitats pròpies d'ATM

Marc Organitzatiu

1. Política de Seguretat.
2. Establiment de rols i responsabilitats (matriu RACI).
3. Normativa de Seguretat:
 - Ús correcte d'equips, serveis i instal·lacions
 - Ús indegut
 - Responsabilitats per incompliments
4. Procediments de Seguretat.

5. Procés d'autorització dels elements del sistema d'informació.
6. Instruccions i guies Tècniques de Seguretat del CCN.

Marc Operacional

1. Document d'Anàlisi de Riscos.
2. Anàlisi de Riscos amb PILAR.
3. Pla de Tractament del Risc.
4. Document que descrigui les instal·lacions:
 - Àrees
 - Equips
 - Xarxes Internes
 - Connexions a l'exterior
 - Punts d'Accés al Sistema
 - Sistemes de Seguretat existents
5. Procediment de Gestió de la Documentació.
6. Informes d'auditories internes.
7. Registre de seguiment d'accions correctives i de millora detectades en auditories.
8. Document que descrigui els processos de seguretat.
9. Procediment per a adquisició de nous components del sistema.
10. Document/s de Gestió de la Capacitat.
11. Procediment de Control d'Accés: identificació, requisits, segregació de funcions, gestió de permisos, autenticació i registre d'accessos.
12. Inventari d'Actius.
13. Procediment de bastionat.
14. Procediment de gestió de configuracions.
15. Pla de manteniment.
16. Procediment de control de canvis.
17. Procediment de gestió d'incidents.
18. Procediment de gestió de claus criptogràfiques.
19. Anàlisi de Riscos associats als proveïdors externs.
20. Procediment de control de compliment de serveis externs.
21. Anàlisi d'Impacte (BIA).
22. Procediment que descrigui disponibilitat de mitjans alternatius.
23. Mètriques del sistema: descripció, responsable de mesurament i registre de mètriques.

Mesures de Protecció

1. Document que descrigui la seguretat a les instal·lacions.
2. Document que descrigui la seguretat de les persones.
3. Pla de Conscienciació.
4. Pla de Formació.
5. Normativa de caracterització i seguretat del lloc d'usuari.
6. Procediment de deures i obligacions.
7. Procediment d'establiment de canals de comunicació segurs.
8. Procediment d'etiquetatge de suports d'informació.
9. Procediment de control de suports d'informació.
10. Registre de transportistes autoritzats.
11. Procediment d'esborrat i destrucció segura de suports.
12. Normativa de seguretat sobre desenvolupament d'aplicacions.
13. Pla de proves d'aplicacions.

14. Procediment d'identificació de dades personals.
15. Documentació relativa al tractament de dades personals.
16. Procediment de qualificació d'informació i identificació de responsabilitats.
17. Procediment d'etiquetatge i tractament d'informació.
18. Política de signatura electrònica.
19. Procediment d'esborrat de metadades en documents.
20. Procediment de Backup.
21. Procediment de protecció del correu electrònic.
22. Procediment de protecció de serveis web.
23. Procediment de desenvolupament segur.
24. Procediment de gestió de la capacitat.
25. Normativa de protecció contra denegació de servei.

Formació

1. Pla de Formació.
2. Pla de Conscienciació.
3. Informes de seguiment dels plans de formació i conscienciació.

Auditoria Interna

1. Pla d'auditories.
2. Informe d'auditories.
3. Pla d'acció per corregir les no-conformitats.

Informes

1. Informes de seguiment setmanals durant la Fase I.
2. Informes de seguiment mensuals durant la Fase II.
3. Informes de seguiment setmanals durant la Fase III.
4. Quadre de comandaments actualitzat amb l'estat actual i objectiu d'adequació a l'ENS, on consultar la llista de requisits pendents, grau d'implementació, incidències, etc,...

Per al desenvolupament del servei és imprescindible realitzar totes aquelles tasques conforme al que està disposat a les guies CCN-STIC per tal d'assolir l'adequació a l'ENS i es recomana fer ús de les eines INES, AMPARO i PILAR, essent recomanable l'ús de qualsevol altra eina del CCN-CERT que pugui ser d'utilitat per a la cobertura dels diferents requisits. No es descarta l'ús d'altres eines de gestió de riscos, sempre que estiguin alineades amb l'ENS, tinguin usabilitat un cop finalitzat el contracte i siguin aprovades per l'ATM.

L'adjudicatari, en l'exercici de la seva funció de gestió documental, facilitarà les polítiques de documentació definides per l'ATM, les plantilles, formularis, etc,... i crearà els lliurables requerits.

L'oferta que presentin els licitadors hauran d'abastar la totalitat de la prestació dels 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.

Donada la necessitat d'estar actualitzats a la vigència normativa aplicable al llarg del contracte, la redacció d'aquests plecs podrien entrar en alguna contradicció i/u omissió. Les omissions errònies dels detalls que siguin indispensables per portar a terme els treballs descrits segons l'esperit i intenció exposats en aquestes prescripcions tècniques,

o que, per us hagin de ser realitzades, no solament no eximeix a l'empresa adjudicatària de l'obligació d'executar aquests detalls omesos o erròniament descrits, sinó que, al contrari, han d'executar-se com si haguessin estat complets i correctament especificats.

5. Finalitats i objectius a assolir

Les finalitats a assolir mitjançant la realització d'aquest contracte consisteixen en el compliment del marc normatiu establert per Reial decret 311/2022 de 3 maig pel qual es regula l'Esquema Nacional de Seguretat i les Instruccions Tècniques de Seguretat publicades pel Centre Criptològic Nacional, dels sistemes i serveis de tecnologia de la informació de l'ATM i de la seva cadena de subministrament. Així com posar a disposició de l'ATM de les eines necessàries per al manteniment del compliment en el futur.

Amb la finalitat de què els licitadors puguin dimensionar les ofertes, s'informa, amb caràcter orientatiu, que el nombre de serveis essencials sobre els que es centraran les tasques d'adequació, són aproximadament una cinquantena, distribuïts en serveis corporatius per a l'administració de l'ATM i serveis a la ciutadania.

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'empresa adjudicatària durà a terme una Planificació detallada que garanteixi el compliment dels objectius globals del projecte. Aquesta planificació haurà de ser aprovada per l' ATM.

En el termini de quinze dies després de l'adjudicació, l'empresa adjudicatària del servei haurà de lliurar un document en el qual es reflecteixi una descripció funcional detallada dels treballs a desenvolupar, que es plasmarà en un document interpretable amb facilitat per usuaris aliens al sistema, document que haurà de ser aprovat l' ATM. Així mateix, l'empresa adjudicatària lliurarà un calendari de detall de l'execució del projecte que inclourà abast, dependències, riscos i durada de les diferents tasques.

L'ATM garantirà a l'empresa adjudicatària les vies de comunicació amb usuaris i actors del sistema quan resulti necessari per disposar de la informació requerida per a l'execució del servei.

6.1. Equip de treball

Les empreses adjudicatàries hauran d'adscriure a l'execució del contracte com a mínim, els mitjans personals que estimin necessaris per a l'execució del contracte i que seran valorats.

Per la naturalesa del projecte i la profunda repercussió que tindrà sobre la seguretat dels sistemes de l'ATM, és imprescindible comptar amb mitjans

personals que comptin amb l'adequada formació tècnica en l'àmbit de la seguretat TIC, així com experiència contrastada en compliment similars als demandats en aquest plec de prescripcions tècniques.

Amb la finalitat de poder garantir la qualitat del servei objecte de la present licitació, l'equip de treball adscrit al mateix per les empreses licitadores ha de ser configurat almenys per:

- Cap de projecte
- Consultor de seguretat sènior
- Consultor de seguretat

Requisits formatius:

- Disposar de titulació universitària de Telecomunicacions o Informàtica o equivalent.

Requisits d'experiència:

- Disposar d'experiència professional en projectes de seguretat:
- Disposar d'experiència en implantació de mesures de seguretat ENS.
- Almenys un dels 3 perfils haurà de disposar d'experiència en Anàlisi de Riscos amb metodologia MAGERIT i eina PILAR.

Per altra banda, es requerirà disposar d'un equip especialitzat en consultes legals: Atesa la necessitat de que participi personal especialitzat en aspectes de caràcter legal, com: definició de l'abast del compliment de l'ENS a l'ATM amb els seus proveïdors, que formen part de la cadena de subministrament, identificació de matrius de responsabilitat, etc, s'ha inclòs un requeriment per que l'adjudicatari disposi d'una bossa de 30 hores per aquesta funció, per a la totalitat del contracte.

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.

L'equip mínim que l'empresa posa a disposició del projecte s'ha de mantenir al llarg de la vigència del contracte. Excepcionalment, en cas que fos necessària la substitució d'algun dels perfils que componen l'equip mínim adscrit al contracte durant l'execució del mateix, l'ATM haurà d'acceptar prèviament aquesta substitució, validant que el nou perfil compleix el mateix nivell de solvència tècnica o superior, i que haurà d'estar operatiu en un màxim de tres setmanes.

Les persones designades per exercir aquest contracte disposaran per part de les empreses adjudicatàries dels mitjans tècnics necessaris per al desenvolupament de les seves tasques, inclòs ordinador personal i 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.

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.

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 present 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.

L'execució del contracte podrà requerir puntualment la realització de jornades laborals de forma presencial a les oficines de l'ATM, segons estableixi l'ATM d'acord a la màxima eficiència per a la prestació del servei.

Als efectes anteriors, s'avaluarà el seguiment i el control del compliment de cada requeriment tècnic de la següent manera:

- A l'inici del servei, es mantindrà una reunió entre l'ATM i el contractista on s'identificaran rols i responsables i s'aprovarà la planificació i calendari proposats per l'empresa adjudicatària per al desenvolupament del servei.
- Al llarg del desenvolupament del servei:
 - Fase I – Definició del Pla d'adequació
Es mantindran reunions operatives setmanals on:
 - Es requeriran informes de seguiment setmanals de l'estat del servei.
 - Es repassarà l'estat dels treballs planificats, identificant les fites complertes i lliurables cobertes.
 - S'identificaran els riscos detectats, el seu impacte i les mesures de mitigació oportunes.
 - Fase II – Execució del Pla d'adequació
Es mantindran reunions mensuals on:
 - Es requeriran informes de seguiment mensuals de l'estat del servei.
 - Es repassarà l'estat del pla d'acció, els treballs planificats, identificant les fites complertes i lliurables cobertes.
 - S'identificaran els riscos detectats, el seu impacte i les mesures de mitigació oportunes.
 - Fase III – Auditoria
Es mantindran reunions operatives setmanals on:
 - Es requeriran informes de seguiment setmanals de l'estat del servei.
 - Es repassarà l'estat dels treballs planificats, identificant les fites complertes i lliurables cobertes.
 - S'identificaran els riscos detectats, el seu impacte i les mesures de mitigació oportunes.

8. Calendari de treball i durada del Contracte

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 contravinquin les condicions del contracte.

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.

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.

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.

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

9.2.3. 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.

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.

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

Signat electrònicament