ATM Àrea de Barcelona
Autoritat del Transport Metropolità

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

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

EXTERNALITZACIÓ CISO (FASE II) EN EL MARC DEL PLA DE RECUPERACIÓ, TRANSFORMACIÓ I RESILIÈNCIA - FINANÇAT PER LA UE - NEXT GENERATION EU" [1]

(Exp. C-32/2023)

Octubre 2024

11 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".

.

Next Generation Catalunya

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

ÍNDEX

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Número d'expedient: C-32/2023

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.

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.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

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.

L'ATM ja disposa d'un rol de CISO ("Oficial de Seguretat de la Informació") contractat des de 2022, col·laboració finançada amb els Mecanisme de Recuperació i Resiliència (MRR). Per assolir els objectius d'aquest contracte en curs, s'ha analitzat la situació de la seguretat a l'ATM i dissenyat un pla de millora, que ha derivat amb la planificació d'activitats a diferents àmbits d'actuació: operacional, de gestió i compliment. Un dels objectius d'aquest plec es la d'assegurar a l'ATM la continuïtat del servei del CISO fins a la finalització de d'aquestes activitats, per realitzar el seu seguiment i garantir que es desenvolupen en els termes i objectius establerts, així com col·laborar amb la consolidació d'un sistema prou madur de sistema de gestió de la seguretat de la informació (SGSI) i que es compleix el marc normatiu de l'ATM en ciberseguretat.

Aquest plec també inclou els serveis 24x7x365 per a realitzar funcions operacionals del Sistema de monitorització, Gestió d'esdeveniments, Informació de seguretat i també serveis propis d'un SOC (*security operations center*) amb capacitat de resposta (CSIRT), principalment Servei de gestió i configuració de seguretat, així com la Resposta davant d'incidents.

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'"Externatització del CISO (Fase II)" 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

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

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.

Les fites i objectius del contracte són les següents:

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 incomplert 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

El present plec té per objecte la prestació d'un servei de CISO, amb la particularitat de garantir la continuïtat de les accions iniciades a l'actual servei de CISO (contracte en vigor, exp. C-37/2021). Per això haurà de monitoritzar i coordinar l'execució de les activitats promogudes des de l'àmbit de seguretat, per garantir que la seva execució es realitza amb els termes acordats.

El contracte de l'actual servei de CISO té prevista la seva finalització el 4 de febrer de 2025.

Donat el cas de que es produeixi un canvi d'adjudicatari del contracte en curs, expedient C-37/2021, amb el d'aquesta licitació, expedient C-32/2023, s'assegurarà el traspàs de coneixement amb un període mínim de dos mesos, durant els quals el CISO sortint, informarà al CISO entrant, de les infraestructures de l'ATM, així com de totes les accions de ciberseguretat en curs o pendents d'executar. Aquesta tasca de transferència de coneixement serà planificada pel CISO sortint, l'execució serà responsabilitat del nou adjudicatari qui informarà setmanalment del seu avanç.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Amb aquesta licitació, l'òrgan de contractació també pretén cobrir les necessitats de monitoritzar els sistemes d'informació de l'ATM contra accessos no autoritzats, així com gestionar els incidents (SOC) i la resposta (CSIRT) que impedeixi comprometre la confidencialitat, integritat i disponibilitat de les dades que són emmagatzemades, processats i transmeses.

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**	
		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

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Q2	2026	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 hagués[2].

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 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).

[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.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

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 són les següents.

4.1. Rol de CISO externalitzat

En aquest apartat s'estableixen les tasques i responsabilitats de forma enunciativa, que no exhaustiva, del contractista adjudicatari, que inclouen les pròpies d'un servei de CISO externalitzat:

- Assegurar el compliment i millora contínua del marc normatiu en matèria de seguretat, donant-ne visibilitat.
- Realitzar el seguiment de les activitats en curs i previstes, en l'àrea de seguretat, especialment les del marc dels Mecanisme de Recuperació i Resiliència (MRR).
- Analitzar l'escenari post "MRR", preveient possibles riscos i recomanant mitigacions.
- Generar i implantar polítiques de Seguretat de la Informació a fi de garantir la seguretat i privacitat de les dades.
- Supervisar l'administració del control d'accés a la informació.
- Dirigir i supervisar el compliment normatiu vigent aplicable de la Seguretat de la informació.
- Responsable de l'equip de resposta davant d'incidents de Seguretat de la informació de l'organització.
- Supervisar l'arquitectura de seguretat de la informació de l'ATM.
- Tenir una visió de negoci que comprengui els riscos que afronta l'organització i com tractar-los.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

- Entendre la missió i els objectius de la Casa i assegurar-se que les activitats són planificades i executades per satisfer aquests objectius
- Estar al dia de les necessitats normatives, la gestió de la reputació de l'organització.
- Establir els plans de continuïtat de negoci i recuperació de desastres en l'àmbit de les TIC.
- Proposar les mesures per adequar-se a nous marc normatius que puguin sorgir.

4.2. Sistema de monitorització i gestió d'esdeveniments i informació de seguretat

ATM disposa d'un sistema de gestió d'esdeveniments d'informació de seguretat (Security Information and Event Management), que referirem com a SIEM, que permet la monitorització i la correlació d'esdeveniments de seguretat, integrant les fonts de dades que generin tots els dispositius i sistemes de xarxa de la T-mobilitat, a l'objecte de detectar anomalies de seguretat i generar alertes que permetin l'adequada classificació del nivell d'amenaça de qualsevol dels incidents de seguretat detectats.

El contractista aprovarà les automatitzacions i correlacions a implantar en les eines de ciberseguretat de l'ATM, detallant els casos d'ús a implantar pel subministrador al qual farà proporcionar, com a mínim cada 2 mesos, els registres d'activitat complets en format inter-operable per a la seva anàlisi.

4.3. Servei de gestió i configuració de seguretat i resposta davant d'incidents

Aquest servei comprendrà la gestió de la supervisió de la instal·lació i configuració de tots els elements de seguretat així com la definició de les integracions a proposar.

També comprendrà la direcció proactiva de totes les actualitzacions de maquinari i programari aplicables a tots els sistemes d'acord amb les especificacions dels respectius fabricants i subministradors així com, si s'escau, la direcció de les re-configuracions necessàries per adequar-se a l'evolució dels sistemes existents al llarg del temps en matèria de seguretat.

El contractista disposarà d'un centre d'operacions de seguretat (*security operations center*), en endavant SOC, amb totes les capacitats necessàries per a la prestació del servei. El SOC haurà de disposar de personal especialitzat en la gestió de la seguretat de la informació i d'incidents de seguretat, així com de gestió de la resposta als incidents (CSIRT).

La prestació del servei es realitzarà en règim de 24x7x365 dies i prioritàriament des de centres ubicats en la Unió Europea, complint totes les normes aplicables que es trobin en vigor.

El servei contemplarà la classificació i priorització de les alertes generades pel SIEM i altres sistemes afins, el tractament dels incidents de seguretat que no hagin estat continguts mitjançant configuracions preestablertes en el sistema i la implantació d'un model de millora continua d'acord a les amenaces i vulnerabilitats que poguessin anar succeint durant la durada del contracte.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Amb periodicitat mensual s'elaboraran informes dels incidents de seguretat, classificats per tipologies i nivell de gravetat.

Dintre d'aquest servei es contemplarà la gestió de vulnerabilitats, tant de la infraestructura (comprenent tant les fallades de software com de la configuració) com de totes aquelles aplicacions accessibles des de la xarxa Internet, i les propostes per a la correcció d'aquestes.

El contractista assumirà també la coordinació per a l'activació de mecanismes de seguretat prestats per terceres parts per a l'ATM, en particular el servei d'accions de monitoratge i gestió d'alertes i resposta 24x7x365 (SIEM). El SIEM està contractat amb un altre tercer. La funció de l'adjudicatari d'aquesta licitació es redueix a la coordinació per a l'activació de mecanismes de seguretat, no a la prestació del SIEM.

Finalment el servei contemplarà l'assistència per a la recollida *in situ* d'evidències forenses relatives a incidents de seguretat i la seva custòdia i preservació a efectes legals i/o processals.

Es coordinarà amb l'Agencia de Ciberseguretat de Catalunya i altres centres de resposta davant incidents i entitats de naturalesa similar dins l'administració de la Generalitat de Catalunya i dins l'àmbit del sector del Transport Públic (operadors de transport, administracions titulars, etc.).

L'ATM disposa de la seva política de seguretat que articula la gestió continua de la seguretat i requereix de l'organització i implantació del procés de seguretat alineant la seguretat de la informació amb els objectius de compliment normatiu i de negoci per garantir la continuïtat de l'activitat i la protecció de la informació en un marc de millora contínua

El contractista serà l'encarregat de generar i implantar dites polítiques de seguretat de la informació; garantir la seguretat i privacitat de les dades i dirigir i supervisar tant l'administració del control d'accés a la informació com el compliment normatiu de la seguretat de la informació vigent al llarg del contracte. A tal efecte, l'objectiu a assolir és el compliment normatiu i d'operacions en matèria de seguretat per part de l'ATM.

5. Finalitats i objectius a assolir

Les finalitats a assolir mitjançant la realització d'aquest contracte consisteixen garantir la continuïtat de les acciones iniciades a l'actual servei de CISO.

Amb aquesta licitació, l'òrgan de contractació també pretén cobrir les necessitats de monitoritzar els sistemes d'informació de l'ATM contra accessos no autoritzats, així com gestionar els incidents (SOC) i la resposta (CSIRT) que impedeixi comprometre la confidencialitat, integritat i disponibilitat de les dades que són emmagatzemades, processats i transmeses.

D'aquesta manera l'ATM podrà seguir disposant d'un CISO que pugui dissenyar el marc ideal en la gestió de la ciberseguretat i la protecció de les dades, coordinar la necessitat d'augmentar les eines de ciberseguretat i la seva explotació, el control de les dades de les

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

organitzacions, així com la necessitat d'adaptar-se a les diferents normatives com l'ENS o a estàndards com ISO.

El contractista serà l'encarregat de generar i implantar les polítiques de seguretat de la informació; garantir la seguretat i privacitat de les dades i dirigir i supervisar tant l'administració del control d'accés a la informació com el compliment normatiu de la Seguretat de la informació. A tal efecte, l'objectiu a assolir és el compliment normatiu i d'operacions en matèria de seguretat (ENS, NIS) per part de l'ATM.

A més a més, és el responsable de dirigir l'equip de resposta davant d'incidents que es produeixin en l'àmbit de Seguretat i està al càrrec de l'arquitectura de seguretat de la informació de l'organització.

6. Requeriments tècnics generals obligatoris de la prestació i/o rendiment o exigències funcionals de la prestació

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

Tasques bàsiques a realitzar:

- Dirigir, orientar i coordinar l'estratègia de seguretat
- Definir la normativa de seguretat i procurar que es compleixi
- Prevenir, detectar i analitzar vulnerabilitats
- Establir i implementar polítiques relacionades amb la seguretat
- Informar i reportar a direcció
- Garantir la privacitat de les dades de l'ATM
- Alinear la seguretat amb la continuïtat de negoci
- Controlar i gestionar els recursos del servei objecte del contracte

Detall de l'equip que prestarà el servei:

Perfil	Experiència / Coneixements
Rol de CISO externalitzat	• **Titulació:** Nivell grau en enginyeria informàtica, telecomunicacions o equivalent • **Experiència:** Mínima de 5 anys en l'àmbit de la gestió de la ciberseguretat: adequació a marcs normatius com RGPD, ENS, i implementació d'estàndards ISO, NIST,... Es valorarà: • **Coneixements:** es valorarà titulacions, certificacions i experiència en l'àmbit de la ciberseguretat i de l'adequació a normatives a l'Administració Pública.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Servei 24x7x365	• Capacitació de coneixements, experiència, formació en seguretat de sistemes de la informació i/o telecomunicacions i certificació del servei.

Més enllà dels requisits mínims que ha de complir l'equip humà, es valorarà l'experiència del perfil CISO .

Tant el perfil CISO com l'equip assignat al servei 24x7x365 (SOC), han de disposar de coneixements legals de l'àmbit de l'objecte del contracte, concretament en relació a la normativa al compliment de l'ENS, així com experiència en tots aquells requisits de servei definits.

Mentre duri la vigència del contracte l'ATM proporcionarà les eines i els equips informàtics i els accessos necessaris per la realització del treball del perfil serveis CISO, en el benentès que la resta de recursos necessaris per a la prestació dels serveis (SOC propi) seran proporcionats pel propi contractista.

La persona designada per exercir el perfil de CISO 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.
per a l'admissió de les propostes.

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 del CISO, 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.

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 aquest plec.

L'adjudicatari designarà al perfil que exercirà les funcions del CISO com a 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.

En la fase inicial s'analitzarà el model de Sistema de Gestió de la Seguretat de la Informació establert, així com el seu grau de maduresa i el grau de compliment del seu marc normatiu.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

En la fase següent s'analitzarà l'estat de les activitats en curs, amb especial cura amb la identificació de riscos d'execució, finalització, etc.

La direcció dels controls organitzatius inclouran: la coordinació de tots els agents, interns i externs a l'ATM que tinguin relació amb la seguretat i ciberseguretat, assignació de responsabilitats, polítiques i supervisió, estructuració dels procediments d'informació, etc.

A banda de amb l'ATM, en nom de qui exercirà el seu rol, el CISO es coordinarà estretament amb l'Agència Catalana de Ciberseguretat (ACC) i el CTTI de la Generalitat de Catalunya i qualsevol altre ens d'ordre superior a l'ATM que en matèria de Ciberseguretat sigui preceptiu i/o necessari.

La disponibilitat del contractista és 24x7x365 per atendre qualsevol incident i liderar-ne l'escalat de responsabilitat, tot i que la jornada de desenvolupament del seu rol s'emmarca dins l'horari de les oficines de l'ATM.

El contractista haurà de lliurar mensualment un informe on reculli les tasques i intervencions realitzades. Aquest informe es presentarà juntament amb la factura.

En tot moment el contractista estarà subjecte i exercirà el servei objecte d'aquesta contractació tenint en compte la perspectiva mediambiental, social, laboral i d'innovació que s'escaiguin en el marc de les funcions d'aquest contracte.

Pel CISO, l'execució del contracte es durà a terme a les dependències, calendari laboral i horari de l'ATM. El tècnic tindrà a possibilitat d'executar les jornades laborals de forma presencial i teletreball, segons les normes de l'ATM i dels requeriments del lloc de treball. El desenvolupament de les tasques del SOC no es realitzaran des de dependències de l'ATM.

8. Calendari de treball i durada del Contracte

S'estableix una durada del present contracte de 12 mesos. En cas que la seva formalització sigui posterior al dia 20 de juny de 2025, el contracte finalitzarà a 20 de juny del 2026.

Els treballs es realitzaran d'acord amb el calendari del programa de treball presentat en l'oferta i que passarà a ser part integrant del contracte d'adjudicació.

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 director 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.

El termini màxim d'execució de la prestació del servei d'aquest contracte serà de 12 mesos. Tal com s'ha definit al punt 4, a banda dels aspectes relacionats amb els requeriments tècnics generals obligatoris de la prestació i/o rendiment o exigències funcionals de la prestació, l'adjudicatari es responsabilitzarà de tasques de gestió, millores, ajustos i aspectes de manteniment que puguin sorgir, fins a la data fi d'execució 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.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

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 servei 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.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

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 subministrament d'aquests contractistes, en la mesura que sigui necessari i d'acord amb els resultats de la corresponent anàlisi de riscos.

ATM, considera necessari que els proveïdors que vagin a concórrer a aquesta licitació hauran d'estar en condicions d'exhibir la corresponent Declaració o Certificació 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, per a la categoria de seguretat BASICA, o superior, dels sistemes que intervinguin en la prestació dels serveis indicats, així com mantenir la conformitat en vigor durant la vigència del contracte. Aquesta declaració o certificat de conformitat amb l'ENS ha d'abastar l'àmbit objecte de la contractació.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

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. S'estableix l'assignació de l'adjudicatari, com a data límit per l'entrega de la Declaració o Certificats de Conformitat del ENS.

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.

La documentació a lliurar per l'adjudicatari, inclou el Pla de seguretat. Un dels aspectes fonamentals a incloure en aquest document es el model de gestió que es realitzarà a les fases de disseny i implantació, per assegurar la conformitat de la plataforma, amb el marc de compliment normatiu, a la fase d'explotació.

9.3. Seguiment

L'adjudicatari assignarà un responsable de seguretat i protecció de dades per tractar els temes de ciberseguretat. L'adjudicatari inclourà en el Pla de seguretat, un model de seguiment de la ciberseguretat en funció de la fase del projecte.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

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.

La proposta tècnica haurà d'incloure, per una banda tant experiència com formació i coneixements addicionals (als requeriments mínims) del perfil CISO, així com una descripció de la metodologia de treball de l'expert CISO i del suport del SOC 24x7, 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.

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

Signat electrònicament