ATM Àrea de Barcelona
Autoritat del Transport Metropolità

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

Fase III Externalització CISO

(Exp. C-25/2025)

Desembre 2025

Balmes, 49, 6a planta, 08007 Barcelona
Autoritat del Transport Metropolità. NIF: P-5890049-I

ÍNDEX

1. Prescripcions generals

Aquest Plec de prescripcions tècniques té per objecte determinar el contingut i l'abast de les tasques que haurà de desenvolupar l'empresa contractista en aquests serveis i els requisits que ha de complir per ser adjudicatària de la mateixa, així com fixar les condicions tècniques a les quals hauran d'ajustar-se els treballs a realitzar.

Amb aquest objectiu, es descriuen els treballs a realitzar i el seu desenvolupament i es relacionen les matèries que han de servir de base per licitar i garantir la qualitat de les propostes.

Així mateix, es descriuen les característiques i contingut de les ofertes a presentar i els criteris que serviran de base, tant per a l'adjudicació dels treballs com perquè els mateixos siguin acceptats per la direcció de l'assistència tècnica.

La direcció dels serveis i la seva aprovació dependran de l'Àrea de Sistemes i Innovació de l'Autoritat del Transport Metropolità, Consorci per a la coordinació del sistema metropolità de transport públic de l'Àrea de Barcelona, (ATM, d'ara endavant).

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. Context

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

L'Àrea de Sistemes i Innovació té encomanades, entre d'altres, la gestió de les polítiques de seguretat informàtica i de protecció de dades, la dels sistemes de seguretat en xarxa i la dels sistemes corporatius d'autenticació d'usuaris. Aquesta Àrea administra una infraestructura de comunicacions i servidors que proporciona el suport sobre el qual

s'implementen les aplicacions corporatives, es distribueix la informació dels seus serveis i es presten els serveis telemàtics als ciutadans. En consonància amb el principi bàsic de "Línies de defensa" establert en el Reial decret 311/2022 del 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), per assegurar aquestes comunicacions, cal orientar l'estratègia de seguretat cap a una solució d'arquitectura multicapa, consistent a introduir múltiples capes de seguretat que permetin reduir la probabilitat que els sistemes d'informació es vegin compromesos i minimitzar l'impacte si la situació de risc arriba a materialitzar-se.

Per altra banda, la nova Directiva europea de Ciberseguretat, NIS2, fou aprovada el 2023 i es aplicable a tots els Estats membres a partir de 2025 i forma part del pilar central de la resiliència digital d'Europa. És una directiva de seguretat i resiliència, no només tecnològica: afecta processos, governança, cadena de subministrament i responsabilitats de direcció.

L'ATM ja disposa d'un rol de CISO ("Oficial de Seguretat de la Informació") contractat des de 2022, serveis contractats mitjançant els expedients de contractació C-37/2021 i C-32/2023, ambdós finançats amb FONS Europeus del Mecanismes de Recuperació i Resiliència (MRR). Per assolir els objectius d'aquesta prestació, actualment en curs mitjançant el contracte C-32/2023, s'ha analitzat la situació de la seguretat a l'ATM i dissenyat un pla de millora, que ha derivat en la planificació d'activitats a diferents àmbits d'actuació: operacional, de gestió i compliment. Un dels objectius d'aquest plec és la d'assegurar a l'ATM la continuïtat del servei del CISO fins a la finalització d'aquestes activitats, per realitzar-ne 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 que li correspon a l'ATM en ciberseguretat.

L'ATM també ha començat, mitjançant els contractes dels exp. C-27/2023 -relatiu als serveis l'Adequació a ENS- i l'exp. C-28/202 -relatiu als serveis d'Auditoria Continuïtat i DRP- les tasques per adequar-se a la normativa ENS i revisar els seus plans de continuïtat. De cara a poder donar continuïtat als serveis prestats en l'execució d'aquests contractes, cal que sigui reforçada la figura del CISO amb un rol expert en governança, gestió del risc i compliment, -l'acrònim GRC en endavant-, per assegurar que l'organització funciona de manera segura, controlada i alineada amb les lleis i normes, els riscos i els objectius estratègics, recolzant, així en les operacions del rol CISO.

Aquest PPT també contempla la prestació dels 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 com a servei de gestió i configuració de seguretat, així com de resposta davant d'incidents.

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

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), que

aplicat a l'Administració Pública i en concret a l'ATM, té com a objectiu orientar l'estratègia de seguretat cap a una solució de garantia de protecció adequada de la informació i els serveis que gestiona l'ens i els proveïdors que hi treballen, per garantir la seguretat de la informació, els sistemes i els serveis electrònics, assegurant que funcionin de manera segura, fiable i resilient.

3. Objecte del contracte

L'objecte del contracte és l'externalització del servei CISO, amb la finalitat de protegir l'organització definint l'estratègia de ciberseguretat, gestionant riscos, garantint compliment normatiu, monitoritzant els sistemes d'informació de l'ATM contra accessos no autoritzats, i liderant la resposta a incidents, amb visió transversal i alineació amb el negoci, de manera que impedeixi comprometre la confidencialitat, integritat i disponibilitat de les dades que són emmagatzemades, processades i transmeses.

El present plec té per objecte la prestació d'un servei de CISO, amb la particularitat de garantir la continuïtat de les acciones iniciades a l'actual servei de CISO (contracte en vigor, exp. C-32/2023). Per això haurà de monitoritzar i coordinar l'execució de les activitats promogudes des de l'àmbit de Seguretat corporativa, per garantir que la seva execució es realitza en els termes acordats. Aquest rol estarà reforçat amb un rol professional expert en governança, risc i compliment, -GRC- juntament amb un servei de Security Operations Center, -SOC-.

Així és necessari mantenir l'actual caracterització del servei d'externalització de CISO i reforçar-les amb un rol professional de GRC (Governance, Risk & Compliance) que combini visió estratègica, comprensió normativa, capacitat tècnica i habilitats de gestió. Assegurar la continuïtat de la correcta execució de les activitats iniciades durant l'actual contracte, identificar punts de millora contínua en les mateixes, aportar bases sòlides per gestió de riscos corporatius, controls interns, auditoria, marcs regulatoris, contractes, gestió legal del risc i polítiques corporatives, son necessitats a cobrir. El contracte també dona continuïtat als serveis implicats amb el Sistema de monitorització, gestió d'esdeveniments, informació de seguretat, Servei de gestió i configuració de seguretat i de resposta davant d'incidents i a les licitacions "C-27/2023 - Adequacio a ENS" i "C-28/2023 - Auditoria Continuïtat i DRP".

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, processades i transmeses.

Per altra banda, es requereix un recolzament al servei i tasques realitzades per la figura del CISO amb un rol expert en Governança, Risc i Compliment (GRC) en el marc normatiu que l'ATM ha de complir que pugui recolzar en les operacions del CISO.

Altrament, és objectiu de la present licitació encaminar l'ATM a l'adequació a la nova Directiva europea de Ciberseguretat, NIS2, de seguretat i resiliència, en la seva vessant no únicament tecnològica, que afecta processos, governança, cadena de subministrament i responsabilitats de direcció.

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 i de governança de seguretat més apropiades per al servei d'acord amb l'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

El CISO és la figura que protegeix l'organització definint l'estratègia de ciberseguretat, gestionant riscos, garantint compliment i liderant la resposta a incidents, amb visió transversal i alineació amb el negoci.

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:

– Alinear i dirigir la Ciberseguretat de l'ATM amb marcs normatius que li corresponen, comprenent la missió i els objectius de l'ATM i assegurar-se que les activitats són planificades i executades

Dissenyar la continuació de l'estratègia global de seguretat alineada amb el negoci minimitzant qualsevol gap.

– Satisfer aquests objectius garantint la continuïtat i resiliència en el pla de seguretat i el seu full de ruta.

– Recavar una visió de negoci que comprengui els riscos que afronta l'organització, la seva gestió i el pla de continuïtat i auditoria

– Establir polítiques i marcs on l'ATM és responsable d'adequació i compliment (ISO, NIST, ENS, NIS, Zero Trust...).

– Dirigir el programa de gestió de riscos de l'organització i la cadena de subministrament i proveïdors

– Dissenyar i dirigir la protecció de la informació i gestió de vulnerabilitats

– Gestió del SOC i resposta a incidents

– Cultura i conscienciació en Ciberseguretat. Formació, bones pràctiques i sensibilització.

– Revisar arquitectura tècnica i de comunicacions en projectes

– Supervisar les infrastructures de sistemes i l'administració del control d'accés a la informació.

– Integrar seguretat en el cicle de vida del programari (DevSecOps).

– Validar plans de gestió de crisis, continuïtat i resiliència

– Informar a la direcció sobre riscos, incidents i estat de la seguretat a l'ATM

4.2. Rol d'expert en Governança, Risc i Compliment (GRC)

El rol principal d'un GRC és garantir que l'organització és segura, compleix la normativa i gestiona els seus riscos de forma proactiva i ordenada.

En aquest apartat s'estableixen les tasques i responsabilitats de forma enunciativa, que no exhaustiva, del contractista adjudicatari, que inclouen les pròpies d'un expert en GRC

- Assessorar el CISO i l'ATM en matèria de normatives.

- Assegurar que l'organització opera de forma coherent amb la seva estratègia.

- Coordinar àrees i assegurar que tots segueixen les mateixes regles.

- Detectar riscos operatius, tecnològics, legals de ciberseguretat.

- Avaluar-hi l'impacte i probabilitat.

- Organitzar i assegurar el compliment de normatives aplicables (GDPR, ENS, NIS2, ISO, directrius del CCN...).

- Gestionar auditories internes i externes.

- Definir controls, proves i evidències.
- Donar suport al CISO en la proposta de plans de mitigació i supervisar que es compleixin.
- Liderar el servei de gestió i configuració de seguretat i resposta davant d'incidents" descrit en el punt 4.4 d'aquest document en coordinació amb el CISO.
- Recolzar el CISO en tot allò que requereixi en el marc de gestió de la seguretat, gestió de riscos i compliment.

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

L'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 de les eines a contractar (objecte d'una altra licitació) al qual farà proporcionar, com a mínim cada 2 mesos, els registres d'activitat complets en format interoperable per a la seva anàlisi.

4.4. 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.

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, no inclosos en aquest contracte, prestats per terceres parts per a l'ATM, en particular el servei d'accions de monitoratge i gestió d'alertes i resposta 24x7x365 (SIEM), no inclòs en aquesta licitació. 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 referència i resposta davant incidents i entitats de naturalesa similar dins l'administració de la Generalitat de Catalunya i dins l'àmbit de l'ecosistema d'influència de l'ATM: administracions titulars (operadors de transport, etc.).

L'ATM disposa de la seva Política de Seguretat que articula la gestió continua de la seguretat i requereix de l'organització la implantació del procés de seguretat i auditoria, 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 les polítiques de seguretat de la informació que s'escaiguin; 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.

En cas que en un futur es torni a licitar l'objecte del present contracte ,l'adjudicatari del present contracte, expedient C-25/2025, caldrà que dugui a terme 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.

5. Finalitats i objectius a assolir

Les finalitats a assolir mitjançant la realització d'aquest contracte consisteixen en garantir i consolidar la continuïtat de les accions ja iniciades per l'actual servei de CISO, així com assegurar la correcta execució de noves necessitats sorgides a aquest respecte.

Amb aquesta licitació, l'òrgan de contractació també pretén complementar 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 requerit 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 organitzacions, així com adaptar-se a les diferents normatives com l'Esquema Nacional de Seguretat, les polítiques de govern de la seguretat aplicables a l'ATM com a organització de sector públic de la Generalitat de Catalunya o a estàndards com ISO aplicables.

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, tot allò normatiu aplicable) 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, de control del risc, de recuperació i continuïtat
- Definir la normativa de seguretat i procurar que es compleixi

- Prevenir, detectar i analitzar vulnerabilitats
- Establir i implementar polítiques i auditoria degudes relacionades amb la seguretat
- Informar i reportar a direcció
- Garantir la seguretat en 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
- Dissenyar programes de formació i conscienciació a l'ATM

Requeriments mínims d'equip humà:

Perfil	Experiència / Coneixements
Rol de CISO externalitzat	• **Titulació:** Nivell grau en enginyeria informàtica, telecomunicacions o equivalent • **Experiència:** Mínima de 5 anys d'experiència professional en l'àmbit de sistemes tecnològics Es valorarà: • **Coneixements:** es valorarà titulacions, certificacions i experiència en l'àmbit de la ciberseguretat.
Rol d'expert en GRC	• **Titulació:** Mínim cicle formatiu de grau superior o titulació de grau universitari de l'àmbit d'informàtica i comunicacions, dret, administració i gestió o similars. • **Experiència:** Mínima de 3 anys d'experiència professional en l'àmbit de sistemes tecnològics Es valorarà: • **Coneixements:** es valorarà titulacions, certificacions i experiència en l'àmbit de la ciberseguretat i de govern, gestió de riscos i compliment.
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 tant del perfil CISO i de l'expert en GRC,

Tant el perfil CISO com l'expert en GRC i l'equip assignat al servei 24x7x365 (SOC) han el disposar de coneixements legals de l'àmbit de l'objecte del contracte, concretament en

relació a la normativa relativa al compliment de l'ENS, la NIS, així com experiència en tots aquells requisits de servei definits.

Durant 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 i del perfil expert en GRC, en el benentès que la resta de recursos necessaris per a la prestació dels serveis (SOC propi) seran proporcionats pel propi contractista.

Les persona designades per a exercir els perfils de CISO i de GRC disposaran 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.

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 o del GRC, 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 com a interlocutor únic amb l'ATM 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.

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.

Amb periodicitat mensual el contractista elaborarà un informe de seguiment, identificant les activitats, el cicle de resolució dels incidents de seguretat, classificats per tipologies i nivell de gravetat, de forma genèrica però oberts a adequar-lo amb la informació que en el seu moment sigui requerida per l'ATM.

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.

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 i l'expert GRC l'execució del contracte es durà a terme a les dependències, calendari laboral i horari de l'ATM. Les jornades laborals s'executaran de forma presencial i en teletreball, segons les normes de l'ATM i dels requeriments necessaris que disposi l'ATM. El desenvolupament de les tasques del SOC no es realitzaran des de dependències de l'ATM.

L'Adjudicatari haurà de facilitar, en temps i forma, la informació que li sigui requerida per acreditar el compliment de les 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.

8. Calendari de treball i durada del Contracte

S'estableix una durada del present contracte de 1 any, amb possibilitat de 2 pròrrogues per un termini d'un any cada pròrroga.

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.

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 del contracte per part d'ATM 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 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.

9.3. 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, per exemple, 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

9.4. 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.

L'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 BÀSICA, 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.

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 de l'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.

9.5. Seguiment

L'adjudicatari assignarà un responsable de seguretat i protecció de dades per tractar els temes de ciberseguretat. L'adjudicatari inclourà en el full de ruta de seguretat, 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.

La proposta tècnica haurà d'incloure una descripció de la metodologia de treball, dels serveis a prestar que haurà d'incloure també el 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.

Inclourà també la titulació addicional i experiència dels perfils CISO i GRC a adscriure a l'execució del contracte.

Joaquim Colomé Batlle
Cap d'Unitat de l'Àrea de Sistemes i Innovació

Signat electrònicament