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, dels serveis de:

Ciberseguretat preventiva: Proves de Penetració

(Exp. C-38/2022)

Juny 2024

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-38/2022

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

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

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

Dins de l'abast d'aquest projecte es troba la contractació relativa als serveis del "Servei de Proves de Penetració" objecte de licitació d'acord amb allò previst als presents plecs.

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

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

1. Context

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

L'Àrea de Sistemes i Innovació té encomanades, entre d'altres, la gestió de les polítiques de seguretat informàtica i de protecció de dades, la dels sistemes de seguretat en xarxa i la dels

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

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 tal de millorar la seguretat i la qualitat del servei prestat al ciutadà, l'ATM es requereix la realització de proves de penetració als seus sistemes d'informació que permetin identificar, analitzar i proposar accions de mitigació de les vulnerabilitats que hi puguin ser presents.

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

2. Fites i objectius

Les fites i objectius del contracte són les següents:

Fita 1: Es preveu la finalització del projecte abans del 30 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

Aquest plec té per objecte establir les prescripcions tècniques particulars que regiran la realització de la prestació del servei de proves de penetració i definir així les seves qualitats.

L'objecte d'aquest contracte és la implementació d'un servei que dugui a terme una comprovació exhaustiva dels sistemes d'informació amb l'objectiu d'identificar vulnerabilitats que permetrien la penetració no autoritzada d'agents maliciosos, així com la posterior anàlisi i proposta d'accions de mitigació en base als resultats de les anàlisis.

Amb la realització de l'objecte contractual esmentat, l'òrgan de contractació pretén cobrir la necessitat de protegir els sistemes d'informació de l'ATM contra accessos no autoritzats que comprometrien la confidencialitat, integritat i disponibilitat de les dades que són emmagatzemades, processats i transmeses.

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'oferta que presenti l'empresa licitadora ha d'abastar la totalitat de les activitats i funcions especificades en aquest plec i en el plec de clàusules administratives particulars, ja que són totes obligatòries per a l'admissió de les propostes.

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.

Les funcions que haurà de realitzar l'empresa adjudicatària són les següents.

- Durant els vint-i-un mesos d'execució del servei, s'haurà de fer una prova de penetració cada dos mesos que cobreixi diferents abasts que s'exposaran, en llistem alguns d'exemple, malgrat aquesta llista pot variar:

    i. Prova de Penetració Externa:
        1. T-Mobilitat
        2. MotorCloud
        3. ATM
        4. Observatori de la Mobilitat
        5. SAE ATM
        6. Per definir

    ii. Prova de Penetració Interna:
        1. T-Mobilitat
            a. CPD Primari
            b. CPD Secundari
        2. MotorCloud
            a. CPD Primari
            b. CPD Secundari
        3. Xarxa Interna ATM
            a. Centre d' atenció T-Mobilitat
            b. Seu ATM
        4. CPD Operadors de Transports (4 CPDs)

    La presentació de resultats de les proves personalitzades hauran de tenir en compte les característiques específiques de l'arquitectura de sistemes de l'ATM.

- L'adjudicatari haurà de generar un informe per a cada prova en la qual s'inclogui per a cada vulnerabilitat: equip afectat, vulnerabilitat detectada, nivell de severitat, descripció d'impacte sobre l'arquitectura de l'ATM, solució de mitigació i informació d'interès per si l'ATM vol ampliar coneixements/informació sobre la vulnerabilitat.

Les proves tenen les limitacions següents:

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

- No modificar dades del negoci de l'ATM
- No fer denegacions de servei ni accessos que puguin tenir com a conseqüència una caiguda del sistema informàtic objecte de la prova.
- No canviar la configuració del sistema informàtic objecte de la prova.

En funció de l'impacte en la producció, les proves podran ser restringides a horaris de matí, tarda o nit; en dies laborables o en festius o caps de setmana sense cost addicional per a l'ATM, a petició d'aquesta amb un preavís de, almenys, un mes.

En definitiva, les funcions que ha d'assumir l'empresa adjudicatària són les següents:

- Execució anual de les proves de penetració tant externs com interns.
- Presentació de resultats.
- Recomanacions en la mitigació de les vulnerabilitats identificades.

L'oferta que presenti l'empresa licitadora haurà d'abastar la totalitat de la prestació del servei 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.

5. Finalitats i objectius a assolir

Les finalitats i objectius a assolir mitjançant la realització d'aquest contracte són els següents:

- Identificar les vulnerabilitats que permetin accedir de forma no autoritzada als sistemes de l'ATM.
- Analitzar la severitat de les vulnerabilitats identificades que permeti la priorització de les tasques de mitigació.
- Recomanar les accions de mitigació per a la resolució de les vulnerabilitats.

Amb aquest objectiu, es requereix un servei que proporcioni les següents funcionalitats:

- Realització de les proves de penetració als actius de l'ATM.
- Presentació de resultats personalitzats que tingui en compte les característiques específiques de l'arquitectura dels sistemes de l'ATM.
- Generació d'un informe per a cada prova en la qual s'inclogui, per a cada vulnerabilitat: equip afectat, vulnerabilitat detectada, nivell de severitat, descripció d'impacte sobre l'arquitectura de l'ATM, recomanació de solució de mitigació i informació d'interès per si l'ATM vol ampliar coneixements/informació sobre la vulnerabilitat.

El servei tindrà un abast a tota la infraestructura de l'ATM. Inclou els actius exposats a internet i els elements connectats a les xarxes internes. Per l'execució d'aquest contracte ATM no haurà de realitzar cap adquisició d'actius, tota l'actuació es realitzarà amb els recursos de l'adjudicatari, en un model de servei.

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

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

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

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.

- Les anàlisis comprovaran els 65535 ports per equip i serveis que en depenen (multiplataforma).
- Identificació i filtratge al màxim dels possibles falsos positius.
- Anàlisi creuada de les vulnerabilitats relacionades i ajust del nivell de risc en base al conjunt i no de manera individualitzada (port, equip, servei, firmware, etc.).
- Recomanacions personalitzades, en base a l'arquitectura (maquinari, programari, comunicacions) de l'ATM i no genèriques que poden donar les eines comercials.
- Identificació de solucions alternatives en cas de no poder-se aplicar la solució proposada.
- Es garantirà el mínim impacte durant la realització de les proves de penetració.
- Les proves de penetració internes hauran d' analitzar l' arquitectura de la xarxa i les aplicacions web que es trobin incloses en aquesta arquitectura.
- Es considerarà acceptable l'ús d' eines comercials, però es valorarà molt positivament la utilització d'eines addicionals
- Dins de l'abast de les proves de penetració s'haurà de dur a terme com a mínim el següent conjunt de proves per a cada actiu de la xarxa:
    - DoS exòtics, DoS Reflectits, DDoS
    - Anàlisi de ports
    - Identificació i anàlisi de serveis
    - Anàlisi d' aplicacions
    - Anàlisi de protocols de comunicacions
    - Algorismes de xifrat de comunicacions
    - Revisió de Firmware
    - Anàlisi de Sistemes Operatius
    - Firewall Pentesting
    - Anàlisi de protocols file share
    - Anàlisi NAS o Sistemes d' emmagatzematge
    - Anàlisi de vulnerabilitats en BBDDPath Traversal
    - Inclusió Remota de Fitxers
    - Divulgació del codi font - / carpeta WEB-INF
    - External Redirect
    - Server Side Include
    - Cross Site Scripting (Reflected)
    - Cross Site Scripting (Persistent)
    - Fallada per Injecció SQL
    - Server Side Code Injection
    - Remote OS Command Injection
    - Homologació de directoris
    - Buffer Overflow
    - Error de format de cadena
    - CRLF Injection
    - Parameter Tampering
    - Fuita d' informació ELMAH
    - .htaccess Information Leak
    - Regles de recerca activades per a l' Script
    - Source Code Disclosure - Git
    - Source Code Disclosure - File Inclusion
    - Execució remota de codi - Shell Shock
    - Httpoxy - Proxy Header Misuse
    - Vulnerabilitats d' OpenSLL HeartBleed

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

- Desconfiguració de Domini creuat
- Divulgació del codi font - CVE-2012-1823
- Execució remota de codi - CVE-2012-1823
- Fixació de Sessió
- Injecció SQL - MySQL
- Injecció SQL - HSQL
- Injecció SQL - Oracle
- Injecció SQL - PostgreSQL
- Injecció SQL - SQLite
- Injecció SQL - MsSQL
- Injecció SQL avançada
- Cross Site Scripting (Basat en DOM)
- XPath Injection
- XML External Entity Attack
- Padding Oracle Attack
- Expression Language Injection
- Cloud Metadata Potentially Exposed
- Divulgació de codi font - SVN
- Relative Path Confusion
- HTTP Only Site
- Anti-CSRF Tokens Check
- Integer Overflow
- Proxy Disclosure
- Trace.axd Information Leak
- .env Information Leak
- Hidden File Finder
- XSLT Injection
- Mètode HTTP insegur
- HTTPS Content Available via HTTP
- GET for POST
- User Agent Fuzzer
- Injecció de paràmetres HTTP
- Enumeració de nom d' usuari
- Cookie Slack Detector
- SOAP Action Spoofing
- SOAP XML Injection
- Anàlisi de Certificats

Serà necessari que el contractista realitzi la presentació de resultats personalitzats que tingui en compte les característiques específiques de l'arquitectura de sistemes de l'ATM que dependrà de l'arquitectura concreta d'on es facin les proves.

7. Calendari de treball i durada del Contracte

S'estableix una durada del present contracte de 21 mesos, des de la data de formalització del contracte. En cas que la seva formalització sigui posterior al dia 20 de setembre de 2024, 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.

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

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 21 mesos. 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.

8. 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'empresa contractista ha de designar una persona responsable de la gestió de l'execució del contracte, que haurà de garantir la qualitat de la prestació objecte d'aquest plec, i tractar 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.

Aquestes persones s'han de reunir amb una periodicitat mínima de dos mesos per tal de supervisar, controlar i tractar qualsevol aspecte vinculat amb el desenvolupament del contracte, a fi d'assegurar que s'està executat de conformitat amb aquest plec.

L'adjudicatari haurà d'aixecar acta de les reunions que seran revisades per l'ATM prèviament a la seva aprovació definitiva.

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

- Informes de seguiment del calendari de proves de penetració, en el qual s'inclogui, els penetració a realitzar, dates estimades d'inici i finalització, estat del penetració, en el cas que s'hagi executat, nombre de vulnerabilitats per severitat.
- Presentació d'un informe de descripció de les proves que es duran a terme que inclogui:
    - Descripció de l'abast i objecte de la prova.
    - Descripció de les proves que es realitzaran, així com de les eines utilitzades.
    - Horari i durada prevista.
    - Sistemes i serveis implicats.
- Presentació dels informes de resultats de les proves de penetració que incloguin per a cada vulnerabilitat:
    - Equip afectat
    - Vulnerabilitat detectada
    - Nivell de severitat
    - Descripció d' impacte sobre l' arquitectura de l' ATM

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

- Solució de mitigació recomanada
- Informació d'interès per si l'ATM vol ampliar coneixements/informació sobre la vulnerabilitat.

El termini per a lliurar els informes i resta de documentació requerida serà de 10 dies hàbils.

9. Equip de treball

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

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 composen 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.

10. Condicions generals d'execució i ciberseguretat

10.1. 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 finalitzat el termini de durada del contracte. 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

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

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.

10.2. 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.

10.2.1. 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

10.2.2. 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

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

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 estiguin 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 estiguin 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.

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 en 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.

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 és 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.

10.3. 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.

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

El licitador haurà de presentar una proposta tècnica d'acord amb el model de l'annex 1 del PCA.

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

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.

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

Signat electrònicament