



PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGEIXEN LA CONTRACTACIÓ DELS SERVEIS D'ASSESSORAMENT, CONSULTORIA, ASSISTÈNCIA TÈCNICA I JURÍDICA EN MATÈRIA DE PROTECCIÓ DE DADES I DE LA IMPLEMENTACIÓ DE L'ESQUEMA NACIONAL DE SEGURETAT A L' AJUNTAMENT DE MATARÓ.

Primera. Objecte del contracte

L' objecte del contracte és la prestació dels serveis de consultoria, assessorament i assistència jurídica en matèria de protecció de dades personals i la implementació de l' Esquema Nacional de Seguretat (ENS) Ajuntament de Mataró.

Segona. Normativa d' aplicació

Principal normativa aplicable per l' execució del contracte:

Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d' abril de 2016 relatiu a la protecció a les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d' aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglamento General de Protecció de Dades). En endavant RGPD.

Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

Reial Decret 3/2010, de 8 de gener, que desenvolupa l'article 42 de la Llei 11/2017, de 22 de juny, d' accés electrònic dels ciutadans als Serveis públics, i modificat pel Reial Decret 951/2015 pel que fa la regulació de l'ENS

Llei 39/2015, de 1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques.

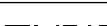
Tercera. Durada del contracte

La durada del contracte serà de dos anys.

Quarta. Definició i característiques del servei

- **Servei de consultoria, assessorament i assistència jurídica i tècnica en matèria de protecció de dades:**

Realització de consultoria, assessorament i assistència jurídica i tècnica, així com adequació i suport dels procediments d'instruccions en matèria de protecció de seguretat de dades personals de

CSV (Codi de verificació Segura)	IV7OEK7SZM4TWVHI5UNFAMCWOU	Data i hora	06/07/2023 13:12:21	
Normativa	Aquest document incorpora signatura electrònica reconeguda d'acord amb la llei 6/2020, 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança			
Signat per	JOAN MASDEU JURNET (CAP SECCIÓ INFORMACIÓ BASE I APLICACIONS CORPORATIVES)			
URL de verificació	https://seu.mataro.cat/verifirma/code/IV7OEK7SZM4TWVHI5UNFAMCWOU	Pàgina	1/6	

conformitat amb l' establert en el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i lliure circulació d'aquestes dades i en la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals. En concret:

- Resolució de consultes tècniques i jurídiques en matèria de protecció de dades personals.
- Assessorament en la revisió i manteniment del Registre d'Activitats de Tractament.
- Manteniment i redacció de clàusules i contractes; adequació de formularis i contractes, per donar compliment a la normativa en matèria de protecció de dades.
- Manteniment i adequació de formularis i altra documentació de l'Ajuntament de Mataró per donar compliment a la normativa en matèria de protecció de dades.
- Establiment de mesures que permetin identificar amb rapidesa els supòsits de violacions en la seguretat de les dades. Supervisió de la gestió i notificació a l'autoritat de control de les violacions de seguretat de dades personals.
- Assessorament continu durant la vigència del contracte.
- Assessorament legal davant les denúncies en matèria de protecció de dades, així com de les sol·licituds d'exercici de drets en base al RGPD.
- Col·laboració en l' actualització de les polítiques de seguretat que afectin a la protecció de dades.
- Realització d'informes jurídics relacionats amb l' aplicació de la normativa de protecció de dades.

- **Implementació de l'Esquema Nacional de Seguretat, que haurà d'incloure controls organitzatius, controls de protecció i controls operacionals:**

A) Controls organitzatius:

-A1) **Directrius de gestió de la seguretat de la informació. Elaborar una política de la seguretat** de la informació basada en marcs normatius i bones pràctiques.

-A2) **Marc de gestió i organització interna de seguretat. Definir un marc de seguretat i/o pla director de seguretat** que inclogui aspectes com la seguretat a la xarxa, la configuració segura de sistemes, la monitorització de l' entorn, la gestió de vulnerabilitats, etc.
Elaborar un procediment per assegurar que els responsables compleixin amb les funcions i responsabilitats associades al seu lloc de treball.

-A3) Seguretat en les relacions amb els proveïdors de serveis. Incorporar en la Política de Seguretat de la informació (SI) clàusules que facin referència a la SI respecte als proveïdors (analitzant la viabilitat sobre l' ús de les clàusules de confidencialitat ja existents pel compliment del present

CSV (Codi de verificació Segura)	IV7OEK7SZM4TWVHI5UNFAMCWOU	Data i hora	06/07/2023 13:12:21	
Normativa	Aquest document incorpora signatura electrònica reconeguda d'acord amb la llei 6/2020, 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança			
Signat per	JOAN MASDEU JURNET (CAP SECCIÓ INFORMACIÓ BASE I APLICACIONS CORPORATIVES)			
URL de verificació	https://seu.mataro.cat/verifirma/code/IV7OEK7SZM4TWVHI5UNFAMCWOU	Pàgina	2/6	



control). Afegint la identificació dels controls de seguretat de la informació per tractar específicament l'accés a la informació de la companyia.

-A4) Seguiment i monitorització dels proveïdors de serveis. Incorporar processos d'avaluació dels proveïdors amb la finalitat d'observar el seu nivell de compliment respecte a requisits de seguretat de la informació i bones pràctiques.

-A5) Compliment de requisits legals i normatius. Identificar la legislació aplicable i els requisits contractuals em matèria de seguretat de la informació. **Elaborar polítiques i procediments de seguretat relatius a l'adquisició, l'ús i llicències de propietat intel·lectual, gestió de llicències i compliment així com polítiques i procediments que contemplin la classificació de tipus de registre, períodes de retenció, mitjans de emmagatzematge, contemplant la possibilitat de destrucció, falsificació i accés no autoritzat en els registres.**

B) Controls de protecció:

B.1) Controls de seguretat en RR.HH: Abans de la contractació . **Elaborar un procediment que desenvolupi les accions realitzades per l'Ajuntament durant la selecció de personal.**

B.2) Control de seguretat en RR.HH: Durant la contractació. **Elaborar un programa de sensibilització i formació en Seguretat de la Informació.**

B.3) Controls de seguretat en RR.HH: Finalització contractació o canvi de lloc de treball.

B.4) Elaborar/revisar polítiques de teletreball.

B.5) Requisits de negoci pel control d'accés (autorització i autenticació en els sistemes). **Definir les necessitats d'accés a cada lloc de treball** basant-se en polítiques tipus "Least Privilege" que assegurin sempre que s'atorga la menor quantitat de privilegis possibles als usuaris.

B.6) Gestió d'accés d'usuari. **Elaborar una política de control d'accés**, on es contempli l'assignació i revocació d'accés dels mateixos per assegurar que l'accés a sistemes i serveis d'informació està basat en les necessitats del negoci i la segregació de funcions adequades basades en rols.

B.7) Responsabilitat de l'usuari final. **Definir un programa formal de conscienciació sobre seguretat IT** que recordi, de forma periòdica, a tots els treballadors, les millors pràctiques de seguretat i les seves obligacions de salvaguardar les credencials que se'ls hi han atorgat.

B.8) Controls criptogràfics. **Definir polítiques** que permetin classificar les informacions en base a aspectes com la confidencialitat, integritat i disponibilitat és el primer pas per saber si és necessari protegir la informació que s'emmagatzema, transmet i/o es processa en els sistemes de l'organització.

CSV (Codi de verificació Segura)	IV7OEK7SZM4TWWHI5UNFAMCWOU	Data i hora	06/07/2023 13:12:21	
Normativa	Aquest document incorpora signatura electrònica reconeguda d'acord amb la llei 6/2020, 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança			
Signat per	JOAN MASDEU JURNET (CAP SECCIÓ INFORMACIÓ BASE I APLICACIONS CORPORATIVES)			
URL de verificació	https://seu.mataro.cat/verifirma/code/IV7OEK7SZM4TWWHI5UNFAMCWOU	Pàgina	3/6	

B.9) Intercanvi d'informació a través de les xarxes públiques. **Definir un marc de control** i les polítiques i procediments necessaris per administrar, de manera segura, la transmissió de qualsevol dada i en especial d'aquelles que siguin confidencials i sensibles a través de les xarxes públiques.

B.10) Requisits de seguretat en sistemes d'informació. **Definir un marc de control i les polítiques i procediments necessaris** relacionats amb l'anàlisi de requisits de seguretat per l'adequació de sistemes i software.

B.11) Seguretat en el desenvolupament i en els processos de suport (cicle de vida de desenvolupament). **Definir un marc de control i les polítiques i procediments necessaris** relacionats amb l'anàlisi de requisits de seguretat per l'adequació de sistemes i software: elaboració d'una política de desenvolupament segura.

C Controls operacionals

C.1 Classificació de la informació. **Definir polítiques i procediments** que permetin classificar la informació en base a aspectes com la confidencialitat, integritat i disponibilitat.

C.2 Manipulació dels suports (dispositius d'emmagatzematge extraïbles). **Establir un marc de control (polítiques i procediments)** que reguli l'ús dels dispositius d'emmagatzematge extraïbles.

C.3 Procediments i responsabilitats operacionals. **Elaboració d'una política de gestió del canvi**, a través de la qual es creïn registres relacionats amb la gestió del canvi, es planifiquin i es gestionin els canvis, i s'avaluin els riscos potencials associats als canvis.

C.4 Protecció contra software maliciós (solucions anti-malware). **Crear un marc de control (polítiques i procediments)** que permetin assegurar que s'identifiquin tots aquells sistemes desplegats considerats com comunament afectats per malware per independentment de si es tracta d'equips corporatius o servidors es procedeixi a la instal·lació d'una solució antimalware.

C.5 Còpies de seguretat. **Elaboració de polítiques i procediments** respecte a les còpies de seguretat dels sistemes.

C.6 Monitorització i registres d'auditoria. **Definir un marc de control (polítiques i procediments)** que assegurin la revisió diària d'aquests sistemes i l'adequada execució dels processos de notificació i escalat en cas de detectar-se una incidència de seguretat.

C.7 Control de software en explotació (actualització i pegat d'equips). **Establir un marc de control (polítiques i procediments)** que permeti:

- Identificar i valorar tots els actius i recursos de l'Ajuntament
- Conèixer el nivell actual d'actualització en cada cas i determinar el risc associat.
- Establir processos que evitin que existeixin equips sense actualitzar o fora del seu cicle de vida.

C.8 Gestió de vulnerabilitats. **Definir un marc de control (polítiques i procediments)** que assegurin que es calendaritza el conjunt d'activitats anteriors amb l'objecte de mitigar el risc de que existeixin vulnerabilitats en els sistemes d'informació.

CSV (Codi de verificació Segura)	IV7OEK7SZM4TWVHI5UNFAMCWOU	Data i hora	06/07/2023 13:12:21	
Normativa	Aquest document incorpora signatura electrònica reconeguda d'acord amb la llei 6/2020, 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança			
Signat per	JOAN MASDEU JURNET (CAP SECCIÓ INFORMACIÓ BASE I APLICACIONS CORPORATIVES)			
URL de verificació	https://seu.mataro.cat/verifirma/code/IV7OEK7SZM4TWVHI5UNFAMCWOU	Pàgina	4/6	



Ajuntament de Mataró

C.9 Gestió d'incidents de seguretat de la informació i millores. **Definir els canals** de comunicació formalitzats per cada esdeveniment o incident de ciberseguretat. **Definir programes de formació i conscienciació** en seguretat informàtica.

Quarta. Criteris d' adjudicació.

1) Oferta econòmica fins a 45 punts

A l'oferta econòmica més baixa s'atorgarà la màxima puntuació. Per la resta d'ofertes, la puntuació s'obtindrà aplicant la següent fórmula:

$$\text{Puntuació} = (\text{oferta econòmica més baixa} / \text{oferta valorada}) * 45$$

2) Experiència de les persones que han d' executar el contracte fins a 45 punts

-Serveis d'assessorament en protecció de dades, fins a 20 punts.

Es valorarà haver realitzat serveis d'assessorament en protecció de dades en Administracions públiques locals de més de 40.000 habitants. S' atorgaran 5 punts per cada servei d' assessorament que s' acrediti haver executat correctament.

Només es valoraran els serveis d' assessorament que tinguin una durada superior a 100 hores.

-Servei de consultoria i assistència per a l'elaboració i implantació del pla d'adequació a l' Esquema nacional de seguretat, fins a 25 punts.

Es valorarà haver realitzat serveis de consultoria i assistència per a l' elaboració i implantació de plans d'adequació a l' Esquema nacional de seguretat en Administracions públiques locals de més de 40.000 habitants. S' atorgaran 5 punts per cada servei que s' acrediti haver executat correctament.

Justificació: L' experiència del personal que ha d'executar el contracte repercuteix en la qualitat del servei.

Les Administracions públiques locals actuen en uns àmbits competencials molt amplis i diversos amb característiques força diferenciades. D'entre tots aquests àmbits n'hi ha diversos, com Policia Local, Benestar Social, àmbit tributari, que tenen les seves especificitats, tant a nivell legal com tècnic i que són molt crítics degut a la tipologia de dades que gestionen. Quan es valora l' experiència en l'àmbit local es busca que les persones que han d'executar el contracte hagin treballat en administracions amb unes competències ben transversals que garanteixin que tenen experiència en el màxim possible d'aquests àmbits

3) Qualificació de les persones que han d' executar el contracte fins a 10 punts

SERVEI DE COMPRES I CONTRACTACIONS
El Carreró, 13. 08301 Mataró
93 758 22 04 – contractacions@ajmataro.cat

5

CSV (Codi de verificació Segura)	IV7OEK7SZM4TWVHI5UNFAMCWOU	Data i hora	06/07/2023 13:12:21	
Normativa	Aquest document incorpora signatura electrònica reconeguda d'acord amb la llei 6/2020, 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança			
Signat per	JOAN MASDEU JURNET (CAP SECCIÓ INFORMACIÓ BASE I APLICACIONS CORPORATIVES)			
URL de verificació	https://seu.mataro.cat/verifirma/code/IV7OEK7SZM4TWVHI5UNFAMCWOU	Pàgina	5/6	

Es valorarà que les persones que hagin d'executar el contracte hagin realitzat estudis de postgrau o màster en protecció de dades. S'atorgaran 2,5 punts per postgrau i 5 punts per màster.

Cinquena. Desenvolupament del servei.

-Serveis d'assessorament en protecció de dades

El temps de resposta màxim a les consultes que es plantegin en el marc de l'assessorament estarà en funció de la seva complexitat. El temps de resolució variarà segons la naturalesa de les qüestions plantejades:

Complexitat baixa: 3 dies hàbils des de la realització de la consulta . Ex: Revisió de clàusules i contractes

Complexitat mitjana: 5 dies hàbils des de la realització de la consulta. Ex: Assessoraments, respostes a requeriments de les Autoritats de protecció de dades.

Complexitat alta: 10 dies hàbils des de la realització de la consulta Ex: Realització informes jurídics.

En cas de consultes que tinguin caràcter urgent els terminis es reduiran a la meitat.

-Elaboració i implantació del pla d'adequació a l'Esquema nacional de seguretat

El termini d'execució per l'elaboració i implantació del pla d'adequació serà d'un any.

Sisena. Pressupost de licitació

El pressupost màxim fixat per l'adjudicació del contracte és de 71.390 euros IVA inclòs pels dos anys de durada inicial del contracte, amb el següent desglossament pressupost net 59.000 euros i 12.390 euros en concepte d'IVA al tipus del 21%.

CSV (Codi de verificació Segura)	IV7OEK7SZM4TWVHI5UNFAMCWOU	Data i hora	06/07/2023 13:12:21	
Normativa	Aquest document incorpora signatura electrònica reconeguda d'acord amb la llei 6/2020, 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança			
Signat per	JOAN MASDEU JURNET (CAP SECCIÓ INFORMACIÓ BASE I APLICACIONS CORPORATIVES)			
URL de verificació	https://seu.mataro.cat/verifirma/code/IV7OEK7SZM4TWVHI5UNFAMCWOU	Pàgina	6/6	