



El secretari accidental,

PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGEIXEN LA LICITACIÓ DEL SERVEI DE CONSULTORIA JURÍDICA I TÈCNICA PER A L'ADEQUACIÓ A LA NOVA LEGISLACIÓ EUROPEA I ESTATAL DE PROTECCIÓ DE DADES PERSONALS I GARANTIA DELS DRETS DIGITALS, PER A LA PRESTACIÓ DEL SERVEI DE DELEGAT DE PROTECCIÓ DE DADES I PER A L'ADEQUACIÓ A L'ESQUEMA NACIONAL DE SEGURETAT I AUDITORIA DEL SISTEMA A L'AJUNTAMENT DE TORTOSA.

Àrea de Serveis Centrals / Unitat de Sistemes d'Informació

Expedient: 2025-INF-C0204-000003

Assumpte: Contractació serveis LOPD i ENS

0 - ANTECEDENTS

El 7 de desembre de 2018 va entrar en vigor la Llei Orgànica 3/2018, de Protecció de Dades personals i garantia dels drets digitals, de 5 de desembre per la qual s'adapta l'ordenament jurídic espanyol al 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 a la lliure circulació d'aquestes dades i completar les seves disposicions, fet que comporta que l'Ajuntament de Tortosa ha de prendre unes mesures específiques per a la seva implementació.

A més, el Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica, determina els requisits tècnics dels sistemes d'informació i alhora preveu la necessitat d'estar en disposició de superar l'auditoria externa de compliment de l'ENS i obtenir el certificat de conformitat.

1- OBJECTE DEL PLEC

L'objecte del present contracte comprèn el servei d'adequació, auditoria, formació i assessorament i assistència jurídica a Llei Orgànica 3/2018, de Protecció de Dades personals i garantia dels drets digitals, de 5 de desembre, i al Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica

El contracte té per objecte la contractació del servei de consultoria jurídica i tècnica per a l'adaptació a la nova legislació de protecció de dades personals i garantia dels drets digitals i a l'Esquema Nacional de Seguretat, auditoria periòdica d'aquests àmbits, accions formatives i de conscienciació i el servei de Delegat de Protecció de Dades. Les funcions que haurà de desenvolupar l'empresa adjudicatària són a grans trets:

Quant a la Llei Orgànica 3/2018:

- Prestació del servei de delegat de protecció de dades.
- Elaborar el Registre d'Activitats de tractament.
- Analitzar les bases jurídiques dels tractaments.
- Anàlisis dels procediments per a detectar els riscos en matèria de Protecció de Dades.



- Identificar i implementar mesures tècniques i organitzatives necessàries per fer front als riscos que es detectin sobre els drets i llibertats dels ciutadans.
- Establir protocols per gestionar i, en el seu cas, notificar fallides en matèria de seguretat.
- Elaborar i dur a terme un pla de formació i conscienciació dels empleats
- Realitzar una auditoria bianual.
- Resolució de dubtes i incidències en aquest àmbit i redacció de documents d'instruccions i recomanacions.

Quant al Reial Decret 3/2010:

- Establir, actualitzar i modificar la política de seguretat de les dades en l'àmbit de l'administració electrònica, que com a mínim inclourà: Organització i implantació del procés de seguretat, anàlisi i gestió dels riscos, gestió de personal, professionalitat, autorització i control dels accessos, protecció de les instal·lacions, adquisició de productes, seguretat per defecte, integritat i actualització del sistema, protecció de la informació emmagatzemada i en trànsit, prevenció davant altres sistemes d'informació interconnectats, registre d'activitat, incidents de Seguretat, continuïtat de l'activitat, millora continua del procés de seguretat.
- Realitzar l'anàlisi de riscos, establert a l'ENS, i elaborar un informe executiu sobre les mesures a adoptar per al compliment de l'ENS.
- Realitzar cada dos anys, com a mínim, l'auditoria de l'Esquema Nacional de Seguretat, tant dels fitxers automatitzats com dels manuals.
- Programar cursos de sensibilització tant per als usuaris com per als administradors dels sistemes d'informació.
- Oferir permanentment el servei d'assessorament i assistència jurídica, incloent l'assistència tècnica en inspeccions dels organismes competents.

A l'efecte de facilitar les ofertes de les empreses interessades, es troben a la seva disposició a les oficines de l'Ajuntament i durant el període de presentació d'ofertes, els documents i dades referides al pla d'acció que es va dur a terme per l'adequació a l'antiga llei LOPD 15/99 i RD 1720/2007, així com els informes d'auditoria bianuals.

En cap cas serà admissible com a causa que impossibiliti l'execució de l'objecte del present contracte l'al·legació per part del contractista del desconexament del volum d'operacions, o de la grandària de l'entitat, o qualsevol altre motiu d'insuficiència d'informació no facilitada a través del present plec.

2- REQUERIMENTS TÈCNICS DEL SERVEI

Adequació a la Llei Orgànica 3/2018, de Protecció de Dades personals i garantia dels drets digitals, de 5 de desembre que adapta 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 a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE, i adequació al Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica .



Les tasques relacionades amb el servei d'Assessoria són:

-Recopilació de la Informació: Enquesta a tots els caps de cada àrea, departament o delegació (si es considera necessari) per realitzar la presa de dades inicial, es tracta d'un inventari tant de hardware com de software.

-Recopilació d'informació sobre els suports d'obtenció de dades personals de cada departament (formularis, contractes, pàgina web, nòmines, fitxes dels treballadors, proveïdors, clients, etc...). També del moviment d'aquestes dades.

-Recopilació d'informació sobre el suport informàtic i magnètic en què estan emmagatzemades les dades.

-Diagnosi mitjançant l'anàlisi de les dades obtingudes, on es determinen les àrees de risc, identificant anomalies.

-Anàlisi detallat dels fitxers i actualització d'aquests.

-Anàlisi detallat de la situació del sistema informàtic, incloent-hi una anàlisi de seguretat d'accessos i localització dels fitxers susceptibles de contenir les dades de caràcter personal. Aquesta primera part té la finalitat de determinar amb la màxima exactitud el grau de confidencialitat de cada fitxer, per tal d'aplicar-li correctament el nivell de seguretat adequat.

-Redacció del Document de Seguretat de l'entitat, estructurat per fitxers de dades de caràcter personal amb l'adequació al tipus de nivell de seguretat establert, que constarà de diversos punts essencials: objecte del document, àmbit de l'aplicació, recursos protegits, funcions i obligacions del personal (responsabilitats en la seguretat i del tractament), normes i procediments de seguretat, gestió d'incidències, gestió de suports, entrada i sortida de la xarxa i telecomunicacions, procediments de còpia de seguretat i recuperació, controls periòdics de verificació i procediment d'exercici dels drets d'accés a les dades.

-Protocols de procediment. Elaboració dels protocols que estableixin de forma clara i resumida les normes bàsiques per als usuaris, perquè el sistema de seguretat sigui viable i funcional

-Redacció de les clàusules. S'elaboraran unes clàusules que hauran de posar-se en tot document que vagi dirigit a la recaptació, compilació i/o altres usos de les dades personals

-Assessorament i assistència jurídiques per tal d'actualitzar els fitxers que hagin sofert alguna modificació. Una assistència jurídica en possibles inspeccions fetes per l'Agència o autoritat de Protecció de Dades, fins a esgotar exclusivament la via administrativa.

-Resolució de dubtes jurídics o tècnics i d'incidències en el decurs de les activitats de l'Ajuntament en matèria de protecció de dades.

Com a auditor:

Auditoria de Protecció de Dades: per tal de verificar la correcta aplicació d'allò establert en el document de seguretat, s'efectuarà una auditoria periòdica, els resultats de la qual es presentaran per escrit i també amb una sessió amb personal de l'Ajuntament.

Quant a la formació:

Pla de formació i cursos de sensibilització. Detecció de les necessitats formatives en l'àmbit de protecció de dades i de seguretat d'aquestes. Davant la necessitat de formació



per part dels membres de l'entitat, es faran sessions de sensibilització en la conveniència d'un control de la seguretat de les dades personals.

Com a delegat de protecció de dades:

- Compliment dels principis relatius al tractament, com els de limitació de finalitat, minimització o exactitud de les dades.

- Identificar les bases jurídiques dels tractaments.

- Valoració de compatibilitats de finalitats distintes a les que van donar lloc a la recollida inicial de les dades.

- Disseny i implementació de mesures d'informació als afectats pel tractament de dades.

- Establir mecanismes de recepció i gestió de les sol·licituds de l'exercici de dret per part dels interessats.

- Valoració de les sol·licituds de l'exercici de dret per part dels interessats.

Proposar a l'òrgan de contractació, si cal, la contractació d'encàrrecs de tractament, inclosos el contingut dels tractaments o actes jurídics que regulin la relació responsable-encàrrec.

- Identificació dels instruments de transferència internacional de dades adequades a les necessitats i característiques de l'organització i de les raons que justifiquin la transferència.

- Disseny i implementació de polítiques de protecció de dades.

- Establiment i gestió dels registres d'activitats de tractament.

- Anàlisi dels riscos dels tractaments realitzats.

- Implantació de les mesures de protecció de dades des del disseny i protecció de dades per defecte adequats als riscos i naturalesa dels tractaments.

- Implantació de les mesures de seguretat adequades als riscos i naturalesa dels tractaments.

- Establir procediments de gestió de violacions de seguretat de les dades, inclosa l'avaluació dels riscos pels drets i llibertats dels afectats i els procediments de notificació a les autoritats de supervisió i als afectats.

- Realització d'avaluacions d'impacte sobre la protecció de dades.

- Implantació de programes en formació i sensibilització del personal en matèria de protecció de dades

- Resolució de dubtes tècnics i jurídics i d'incidències en el decurs de les activitats de l'Ajuntament i elaboració de notes, avisos, circulars o instruccions per al conjunt de la institució o per a unitats, àrees o actors/agents específics.

Quant a l'ENS

- Identificació i valoració dels actius, en especial, els expedients electrònics afectats per l'administració electrònica i dels serveis de tramitació electrònica corresponent.

- Categoritzar els sistemes d'informació —bàsica, mitjana i alta—, atenent a la valoració de la informació i el serveis prestats, tenint en compte els criteris de disponibilitat, autenticitat, integritat, confidencialitat i traçabilitat, definides a l'annex-I) de l'ENS.



-Desenvolupar l'anàlisi de riscos dels actius catalogats, incloent la valoració de les mesures de seguretat existents, utilitzant la metodologia Magerit, del Centro Criptológico Nacional.

-Anàlisi diferencial dels sistemes respecte del compliment de l'ENS i del RD 1720/2007, el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei Orgànica 15/1999, de protecció de dades de caràcter personal.

-Elaborar la declaració d'aplicabilitat, és a dir el document tècnic que defineix les accions a desenvolupar per mitigar els riscos identificats i analitzats, de conformitat amb l'annex-II) de l'ENS.

-Elaborar el preceptiu informe d'insuficiències.

-Elaboració del Pla de millora de la seguretat, sobre la base de les insuficiències detectades, que haurà de fer constar les actuacions a desenvolupar i els seus terminis d'execució.

Implementar el Pla de millora de la seguretat aprovat prèviament per l'òrgan competent, que haurà d'incloure, àmpliament documentat, tots els procediments, normatives, protocols; avaluacions i controls específics i periòdics per correctament: implementar, operar i monotonitzar les mesures de seguretat a través de la gestió continuada de la seguretat, del sistema o sistemes d'informació.

- Exercir el rol de Responsable de Seguretat en el Comitè de Seguretat de la Informació si així es determina en el Document de Seguretat de la Informació.

-En el supòsit de que la categorització del sistema d'informació fos de categoria Bàsica, l'assistència tècnica i jurídica necessària per l'expedició —auto-declaració— per aquesta administració municipal, de la Declaració de Conformitat amb l'Esquema Nacional de Seguretat.

-En el supòsit de que la categorització del sistema d'informació fos de categoria Bàsica però l'Ajuntament volgués obtenir la seva certificació, l'assistència necessària per l'obtenció de la Certificació de Conformitat amb l'Esquema Nacional de Seguretat que expedeixen les entitats certificadores homologades per ENAC —Entitat Nacional d'Acreditació.

-En el supòsit de que la categorització del sistema d'informació fos de categoria mitjana o alta, l'assistència necessària, per l'obtenció de la Certificació de Conformitat amb l'Esquema Nacional de Seguretat que expedeixen les entitats certificadores homologades per ENAC —Entitat Nacional d'Acreditació.

-L'assistència necessària per al compliment de la resolució de data 7 d'octubre de 2016, de la Secretaria d'Estat de les Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat de l'Informe del Estat de Seguretat, que assenyalava que les entitats públiques comunicaran, almenys amb caràcter anual, l'estat de les variables de seguretat del sistema o sistemes d'informació que es troben al seu càrrec.

-Pla de formació.

-L'auditoria de seguretat que regula l'article 34 de RD 3/2010 l'Esquema Nacional de Seguretat.

-Desenvolupar la figura de coordinació entre el Delegat de Protecció de Dades-Responsable de Seguretat i el Cap d'Informàtica i Noves Tecnologies en els treballs a confeccionar segons els rols assignats, és a dir: Responsable de Seguretat i Responsable del Sistema, respectivament, en l'execució de l'esquema.



DOCUMENTACIÓ A LLIURAR

Com a conseqüència dels treballs realitzats l'adjudicatari ha de lliurar la documentació següent:

- Registre d'Activitats de tractaments, mitjançant dos documents, un que presenti el model de realització i un segon que avalui els riscos i que s'ajusti a la guia de seguretat (CCN-STC-803) Esquema Nacional de Seguretat i Valoració dels Sistemes per realitzar l'avaluació del impacte sobre les dades de l'Ajuntament.

- El Pla d'acció, els models tipus de formularis adaptats als requeriments del RGPD, les bases jurídiques de tractaments. Proposició de clàusules per a l'adequació de formularis en matèria de Protecció de Dades.

- Els protocols per gestionar i, en el seu cas, notificar fallides de seguretat.

- Documentació dels tractaments dels riscos considerats alts així com la documentació del procediment per realitzar un impacte de privacitat. Procediments de violacions en la seguretat de les dades personals.

- L'adaptació de contractes anteriors, documentació tipus per a acreditar el consentiment i garantir la possibilitat de revocar-lo. Models tipus per atendre els drets dels ciutadans, habilitant mitjans electrònics. Així com els procediments per exercir els drets de les persones interessades. Polítiques de protecció de dades d'usuaris, proveïdors i recursos humans.

- Material didàctic que permeti la formació als empleats. Aquest es materialitzarà en un manual de formació.

- Resum dels treballs de l'Esquema Nacional de Seguretat. Com a memòria final dels treballs desenvolupats, s'haurà de lliurar en suport electrònic i, si s'escau, en paper, tota la documentació tècnica de les diferents tasques o processos desenvolupats en la implementació de l'ENS.

- Informes d'auditoria de protecció de dades i de l'ENS.

CONDICIONS DE PRESTACIÓ DEL SERVEI

El contracte es prestarà tant a les dependències de l'Ajuntament com des de les oficines de l'empresa adjudicatària. Amb motiu de la realització de l'auditoria, caldrà que personal de l'empresa es desplaci els dies que calgui a les dependències de l'Ajuntament i caldrà fer una presentació de l'informe final també a les mateixes dependències. En cas de suscitar-se algun tema de rellevància o de dificultat especial es poden concertar reunions especials a l'Ajuntament amb personal de l'empresa adjudicatària

L'equip que prestarà el servei hauran d'estar degudament formats i acreditar experiència en els diferents Marcs Normatius i estàndards sobre els quals es desenvolupa el projecte.

L'empresa adjudicatària serà responsable que el seu personal compleixi les normatives legals de seguretat i higiene en el treball i de prevenció de riscos laborals que siguin d'aplicació durant la prestació dels seus serveis i serà igualment responsable dels accidents o malalties que en l'exercici de la seva feina puguin incórrer.



Per al personal de l'empresa adjudicatària del concurs que durant la prestació dels seus serveis tingui accés a fitxers que continguin dades de caràcter personal de propietat de l'Ajuntament, els serà d'aplicació allò que estableix la Llei 3/2018 i les normes de seguretat. Totes les actuacions davant d'una incidència o tasca ordinària seguiran els protocols i els circuits de notificació definits. Els serveis prestats s'ajustaran en tot moment a les exigències establertes per la normativa vigent aplicable.

L'Equip de Treball en tot moment haurà de mantenir les condicions que hagin estat objecte de valoració per l'adjudicatari.

COORDINACIÓ I SEGUIMENT

El contractista designarà un únic Responsable del Servei que actuarà com a interlocutor seu per a qualsevol qüestió relacionada amb l'execució de les prestacions.

L'Ajuntament designarà un responsable per a supervisar i coordinar els treballs fets, exigir els mitjans necessaris per garantir el nivell de servei compromès i solucionar qualsevol dubte que pugui sorgir durant la prestació de serveis objecte d'aquest plec.

L'Equip de Treball no podrà ser modificat en el transcurs del contracte sense el coneixement i autorització prèvia de l'Ajuntament. No obstant això, el contractista, si ho considerés necessari, podrà proposar la substitució d'un o més components de l'Equip de Treball, per altres considerats més idonis.

Tortosa (Terres de l'Ebre), a data de la signatura electrònica
El responsable del contracte

