



**AJUNTAMENT
D'ESPARREGUERA**

AJUNTAMENT D'ESPARREGUERA

Servei assessorament en matèria de protecció de dades i esquema nacional de seguretat

Plec de Prescripcions Tècniques

Expedient núm. 3085-6964/2023

CSV: d1fd9de6-4800-4f07-9ea5-5ec271f2a124
Aquest document és document electrònic segons l'article 27 de la Llei 39/2015, de
1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça
<https://tramits.esparreguera.cat/Ciudadania/ValidarDocuments.aspx>





1. Objecte.....	3
2. Servei Delegat Protecció de Dades.....	3
3. Adequació a l'Esquema Nacional de Seguretat i el seu manteniment.....	6
4. Auditoria ENS.....	7
5. Definició i desenvolupament dels elements mínims a incloure en la planificació de les auditories.....	10
6. Contingut de l'activitat formativa del personal i membres de la corporació.....	11
7. Generalitats.....	12
8. Supervisió, control i seguiment.....	12
9. Temps de resposta.....	12



1. Objecte

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

Aquests plec conté la definició dels requeriments per al servei de delegat de protecció de dades i suport, assessorament i manteniment del compliment de la normativa de gestió de protecció de dades i esquema nacional de seguretat.

La normativa principal aplicable a l'execució d'aquest contracte és:

- 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 Protección de Datos). En endavant RGPD.
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.
- Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- Llei 39/2015, de 1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques
- Altres que siguin d'aplicació.

2. Servei Delegat Protecció de Dades

2.1. Abast

Les tasques intrínseques a l'adaptació i compliment de la normativa de protecció de dades que l'adjudicatari haurà de prestar, són com a mínim les següents:

- Suport als departaments i serveis de la corporació municipal en la gestió relacionada amb els tractaments de dades personals.
- Prestació de la figura del Delegat de Protecció de Dades i tasques especialitzades de suport al mateix.
- Identificar les finalitats i la base jurídica dels tractaments, col·laborar en el manteniment del Registre d'Activitats de Tractament.
- Elaborar la informació dels tràmits i procediments per tal d'atendre en temps i forma, els drets dels afectats.



AJUNTAMENT D'ESPARREGUERA

- Elaborar l'anàlisi de riscos per als drets i llibertats de la ciutadania de tots els tractaments de dades que es desenvolupin quan el nivell de risc ho aconselli i revisar les mesures de seguretat que s'apliquen als tractaments en base a aquest anàlisi.
- Elaborar el procediment d'avaluació d'impacte en la protecció de dades i supervisar la seva realització i compliment.
- Assegurar l'existència, revisió i actualització de la documentació relacionada per tal de garantir el compliment del RGPD.
- Prestar suport a la gestió i notificació de les violacions de seguretat de les dades personals a l'autoritat de control.
- Formar al personal i als membres de la corporació.
- Definir, revisar i/o elaborar els procediments, els protocols i les instruccions aplicables per a la gestió de dades personals.
- Col·laborar en l'elaboració de la documentació de diferents àmbits que afectin a la protecció de dades i que derivi de l'assessorament efectuat pel delegat de protecció de dades.
- Adequació permanent de la normativa interna dels protocols de treball i models de documents als criteris i requeriments de la legislació en matèria de protecció de dades.
- Realització d'auditories internes i de les obligatòries que marca el RGPD.
- Prestació de la figura del Delegat de Protecció de Dades.

2.2. Funcions Delegat Protecció de Dades (DPD).

El DPD és un professional, les funcions del qual s'assenyalen en l'article 39 del RGPD, que s'ocupa de l'aplicació de la legislació sobre privadesa i protecció de dades.

El DPD assumirà com a mínim les següents funcions:

- Informar i assessorar al responsable o a l'encarregat del tractament i als empleats que s'ocupin del tractament de les obligacions que els incumbeixen en virtut del Reglament i d'altres disposicions de protecció de dades de la Unió o dels Estats membres.
- Supervisar el compliment del que es disposa en el Reglament, d'altres disposicions de protecció de dades de la Unió o dels Estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals.
- Oferir assessorament sobre l'avaluació d'impacte relativa a protecció de dades i supervisar la seva aplicació de conformitat amb l'article 35 del Reglament.
- Cooperar amb les autoritats de control i actuar com a punt de contacte amb els interessats.
- Actuar com a punt de contacte de l'autoritat de control per qüestions relatives al tractament, inclosa la consulta prèvia a què es refereix l'article 36, i realitzar consultes, si s'escau, sobre qualsevol altre assumpte.
- Elaborar les respostes a requeriments de l'autoritat de control.
- Elaborar respostes a requeriment de la ciutadania en l'exercici de drets en matèria de protecció de dades de caràcter personal.
- Supervisar la posada en pràctica efectiva de les polítiques de protecció de dades, incloses la formació i l'auditoria.



AJUNTAMENT D'ESPARREGUERA

- Supervisió de l'aplicació de les mesures correctives proposades per a corregir les no conformitats detectades en les auditories obligatòries de compliment de la normativa de protecció de dades de caràcter personal.
- Realitzar el conjunt de tasques i actuacions necessàries per tal d'adequar l'activitat administrativa als nous preceptes legals.
- Identificar les finalitats del Registre d'Activitats de Tractament i mantenir-lo actualitzat.
- Assessorar en la identificació dels contractes que impliquin tractament de dades de caràcter personal i garantir que els contractes es signen i es compleixen.
- Elaborar, revisar o mantenir la informació dels tràmits i procediments per tal d'atendre en temps i forma les sol·licituds relatives als drets dels afectats, al dret d'accés, rectificació, supressió (dret a l'oblit), oposició i limitació al seu tractament.
- Elaborar, revisar i/o mantenir l'anàlisi de riscos per als drets, llibertats de la ciutadania de tots els tractaments de dades que es desenvolupin quan el nivell de risc ho aconselli i revisar les mesures de seguretat que s'apliquen als tractaments en base a aquest anàlisi.
- Revisar i implementar, si s'escau, el procediment d'avaluació d'impacte en la protecció de dades i supervisar-ne la seva realització i compliment.
- Revisió i actualització de tota la documentació relacionada per tal de garantir el compliment del Document de seguretat, Política de seguretat, Manual de funcions i obligacions dels usuaris, nous procediments...
- Supervisió de la gestió i notificació a l'autoritat de les violacions de seguretat de les dades personals a l'autoritat de control. Aquesta tasca compren l'elaboració d'un informe semestral sobre l'estat d'incidents i violacions de seguretat produïts.
- Respondre a les consultes realitzades que seran tramitades pel responsable del contracte, referents a la gestió i tractament de dades de caràcter personal.
- Realització anual d'auditories internes de compliment de la normativa de protecció de dades. Detecció de no conformitats, proposta de mesures correctives i supervisió de la seva aplicació.

El DPD exercirà les seves funcions prestant la deguda atenció als riscos associats a les operacions de tractament, tenint en compte la naturalesa, l'abast, el context i finalitats del tractament. L'exercici de les funcions anteriors comporta:

- Recollir informació per determinar les activitats de tractament
- Analitzar i comprovar la conformitat de les activitats de tractament
- Informar, assessorar i emetre recomanacions al responsable o l'encarregat del tractament.
- Recollir informació per supervisar el registre de les operacions de tractament (Registre de tractament)
- Assessorar en l'aplicació del principi de la protecció de dades per disseny i per defecte.
- Assessorar sobre:
 - si s'ha de dur a terme o no una avaluació d'impacte de la protecció de dades.
 - quina metodologia ha de seguir-se en efectuar una avaluació d'impacte de la protecció de dades.
 - si s'ha de dur a terme la revisió de l'avaluació d'impacte de la protecció de dades.



AJUNTAMENT D'ESPARREGUERA

- o quines salvaguardes (incloses mesures tècniques i organitzatives) cal aplicar per mitigar qualsevol risc per als
 - o drets i interessos dels afectats.
 - o si s'ha dut a terme correctament o no l'avaluació d'impacte de la protecció de dades.
 - o prioritzar les seves activitats i centrar els seus esforços en aquelles qüestions que presentin majors riscos relacionats amb la protecció de dades.
 - o prestar serveis de formació per tal de millorar la implementació de les polítiques de protecció de dades.
- Assessorar al responsable del tractament sobre:
 - o quina metodologia emprar en dur a terme una avaluació d'impacte de la protecció de dades
 - o quines àrees han de sotmetre's a auditoria de protecció de dades interna o externa, o quines
 - o activitats de formació internes proporcionar al personal o els directors responsables de les activitats de tractament de dades i a quines operacions de tractament dedicar més temps i recursos.

Els requisits mínims exigits per prestar les funcions de DPD (habilitació professional) seran:

- Tenir coneixements especialitzats del Dret.
- Pràctica en matèria de protecció de dades.
- Capacitat per a exercir les funcions esmentades en l'article 39 RGPD

3. Adequació a l'Esquema Nacional de Seguretat i el seu manteniment

Amb el suport de la Comissió de Seguretat, el contractista realitzarà les tasques d'assessorament per a l'elaboració de la documentació definida a l'Esquema Nacional de Seguretat (ENS) i la seva implantació a l'Ajuntament. Així mateix, caldrà dur a terme el servei de suport i manteniment continuat del sistema al llarg de tota la durada del contracte.

Aquestes tasques consistiran en l'assessorament per donar compliment a les obligacions establertes al Reial Decret 311/2022, de 3 de maig pel que es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, i que en tot cas inclou:

- Anàlisi de riscos dels nous procediments electrònics i sistemes informàtics que s'incorporin.
- Revisió i modificació dels Procediments tècnics i Política de Seguretat segons els canvis succeïts.
- Tasques de recolzament necessàries per administrar, gestionar i controlar la seguretat de la informació i la protecció de dades a l'Ajuntament.
- Suport online sobre aspectes de l'aplicació de l'ENS a l'Ajuntament: resolució de dubtes i consultes derivades de les tasques habituals de l'Ajuntament en els procediments i mesures establertes.



4. Auditoria ENS

4.1. Objectius

Els objectius de l'Ajuntament d'Esparreguera envers l'Auditoria ENS, a realitzar biennalment a partir de l'inici del contracte i tenint en compte les dades de l'informe de la darrera auditoria són:

- Realitzar l'auditoria ENS d'obligat compliment d'allò que estableix el Reial Decret 311/2022, de 3 de maig, que regula els requisits mínims per acomplir per part de l'Ajuntament d'Esparreguera, ampliar als sistemes de categoria bàsica i de les instruccions específiques aplicables a l'administració pública.

Aquestes auditories es realitzaran de manera ordinària cada dos anys, de manera extraordinària, sempre que es produeixin modificacions substancials en el sistema d'informació, que puguin repercutir en les mesures de seguretat requerides.

Les auditories seran determinades per la Comissió de Seguretat que també en determinarà la seva periodicitat amb l'objectiu de verificar la possibilitat que els controls establerts a través de les mesures de seguretat siguin efectius i que sigui possible garantir la integritat, la confidencialitat i la disponibilitat de les Dades Personals, d'acord amb l'establert al Document de Seguretat.

Es procedirà a estudiar i elaborar el respectiu informe d'auditoria sobre la situació actual de les mesures, processos i procediments organitzatius, tècnics i jurídics

- Realitzar el seguiment de les mesures correctives: L'equip consultor a càrrec del projecte donarà suport en la resolució de les no conformitats segons s'acordi i planifiqui un cop finalitzada l'auditoria.

4.2. Actuacions preparatòries de les auditories

Previ a la realització de les auditories del compliment tant de l'Esquema Nacional de Seguretat com, si cal, en matèria de Protecció de Dades de Caràcter Personal, l'elaboració i preparació de la documentació requerida per concretar la superació d'aquestes i que es concreta, almenys, en la següent:

- Els documents signats per l'òrgan competent corresponent, segons s'estableix en el RD 311/2022, que mostrin el coneixement i l'aprovació formal de les decisions en matèria de política de seguretat.
- L'organigrama dels serveis o departaments afectats, amb descripció de funcions i responsabilitats.
- La identificació dels responsables: de la informació, dels serveis, de la seguretat i del sistema, segons es contemplen en el RD 311/2022.
- La descripció detallada del sistema d'informació a auditar (programari, maquinari, comunicacions, equipament auxiliar, ubicacions i similars).
- Identificació de la categoria del sistema segons l'Annex I del RD 311/2022..



AJUNTAMENT D'ESPARREGUERA

- Els nivells de seguretat definits.
- La Política de Seguretat DPD.
- La Política de Signatura Electrònica i Certificats.
- La normativa de seguretat.
- Descripció detallada del sistema de gestió de la seguretat i la documentació que ho substantia.
- La declaració d'aplicabilitat.
- Les decisions adoptades per gestionar els riscos.
- Relació de les mesures de seguretat implantades.
- Relació de registres d'activitat quant a les mesures de seguretat implantades.
- Informes d'altres auditories prèvies de seguretat relacionats amb els sistemes i serveis inclosos en l'abast de les auditories.
- Informes de seguiment de deficiències detectades en auditories prèvies de seguretat, i relacionades amb el sistema a auditar, si escau.
- Llista de proveïdors externs els serveis dels quals es veuen afectats o entren dins de l'abast de l'auditoria, i evidències del control realitzat sobre aquests serveis.

Aquesta documentació s'elaborarà i prepararà en estreta col·laboració amb la Comissió de Seguretat de l'Ajuntament d'Esparreguera.

4.3. Presentació dels resultats de revisions i prèvies dels informes d'auditoria i del resum executiu final

En qualitat d'assessors dels treballs objecte del contracte esmentats abans, s'hauran de lliurar en suport electrònic i, si escau, en paper:

- a) La documentació revisada, actualitzada i definitiva relativa al sistema de gestió de la seguretat de la informació de l'Ajuntament d'Esparreguera. Aquesta documentació contemplarà almenys la següent informació:
 - o La política de seguretat de la informació
 - o La valoració de la informació
 - o La valoració dels serveis
 - o El document de seguretat
 - o La declaració d'aplicabilitat
 - o L'anàlisi de riscos
 - o La insuficiència dels sistemes
 - o El pla de millora de la seguretat
 - o La política de signatura electrònica
 - o La proposta d'accions correctores o de millora que suposin un cost addicional amb l'anàlisi d'alternatives i costos.



**AJUNTAMENT
D'ESPARREGUERA**

- b) Els informes d'auditoria en matèria de protecció de dades i de l'Esquema Nacional de Seguretat segons el RD 311/2022 els informes d'auditoria seran analitzats per la Comissió de Seguretat perquè adopti les mesures correctores adequades.

L'equip auditor no lliurarà ni concedirà accés a l'informe d'auditoria a tercers diferents dels indicats en el paràgraf anterior, excepte per imperatiu legal, municipal o mandat judicial.

Els informe d'auditoria i/o verificació final haurà de dictaminar sobre l'adequació de les mesures exigides per la normativa d'aplicació, identificar les seves deficiències i proposar les mesures correctores o complementàries necessàries. Haurà, igualment, d'incloure les dades, fets i observacions en què es basin els dictàmens aconseguits i les recomanacions proposades. L'informe inclourà les no conformitats oposades durant la realització dels informes.

Els informes inclouran una opinió sobre si:

- La Política de Seguretat defineix els rols i funcions dels responsables de la informació, els serveis, els actius i la seguretat del sistema d'informació.
- Si escau, si existeixen procediments per a la resolució de conflictes entre dites responsables.
- S'han designat persones per a aquests rols a la llum del principi de "separació de funcions".
- Existeix un sistema de gestió de la seguretat de la informació, documentat i amb un procés regular d'aprovació pe l'adreça.
- S'ha realitzat una anàlisi de riscos, amb revisió i aprovació regular, segons l'establert en les mesures aplicables pel Annex II del RD 311/2022.
- Es compleixen les mesures de seguretat descrites en l'Annex II, sobre Mesures de Seguretat, en funció de les condicions d'aplicació en cada cas.
- Existeix un sistema de gestió de millora contínua.
- S'ha identificat quan una deficiència de seguretat o incompliment, o una millora recomanada està, individualment, relacionada amb ambdues normes, o bé amb una en concret.

En els annexos dels informes es descriuran els detalls i resultats de les proves que permeten arribar a les conclusions de l'informe executiu, agrupant-los pels apartats de l'informe executiu.

L'Informe d'Auditoria es podrà presentar en format audiovisual. No obstant això, aquest informe sempre haurà de lliurar-se en suport documental degudament signat amb signatura electrònica.

- c) Informe executiu final del contracte: Aquest resum executiu inclourà una breu descripció dels treballs realitzats, les recomanacions i les propostes de mesures de millora valorades econòmicament.



AJUNTAMENT D'ESPARREGUERA

En l'informe s'incorporarà un apartat en el qual es realitzi, si cal, una proposta de full de ruta per a la millora del compliment dels diferents normes que és objecte aquest contracte que inclourà una anàlisi econòmica per a cadascun dels diferents escenaris proposats.

5. Definició i desenvolupament dels elements mínims a incloure en la planificació de les auditories

Els elements mínims en els que l'assessorament s'haurà de definir, la planificació de les auditories seran els següents, tenint com a referència així mateix l'Annex II del RD 311/2022, de manera que hauran de ser lliurats els informes, documents i projectes necessaris perquè, prèviament a la realització de la formació i de les auditories, se sotmetin a dictamen i consideració:

- a. Anàlisi i gestió de riscos. Tipus de proves a realitzar: sustentació metodològica de l'anàlisi de riscos realitzat, la seva coherència i documentació, i verificació de l'inventari d'actius. Per a això l'equip auditor pot basar-se, per exemple, en la norma UNEIX 71504 (gestió de riscos informàtics)
- b. El marc organitzatiu i la segregació de funcions. Tipus de proves a realitzar: documentació de les polítiques i procediments (accessibilitat pel personal al que afecta i actualització); la comunicació de les normes, de les responsabilitats i de la conscienciació del personal afectat sobre aquestes normes, polítiques i procediments.
- c. El marc operacional (Control d'Accessos, Explotació, Serveis Externs, Continuitat del Servei i Monitoratge del Sistema).

Tipus de proves a realitzar: avaluació, entre uns altres, de les proves fefaents de la continuïtat del servei, amb inclusió o no dels serveis externs; les autoritzacions i sol·licituds d'accés, el registre i seguiment dels incidents de seguretat; l'adequació dels drets d'accés que considerin la segregació de funcions, avaluació del control de capacitat dels sistemes, els mecanismes de control per a l'accés físic, etc)

- d. La Declaració d'Aplicabilitat que recull tant les mesures de seguretat de l'Annex II del RD 311/2022 que són rellevants per al sistema d'informació subjecte a l'auditoria.

Tipus de proves: la revisió dels registres d'activitat i supervisió; fortaleza de les mesures de seguretat de les comunicacions enfront d'atacs interns o externs, control de canvis en aplicacions i sistemes, compliment de contractes de propietat intel·lectual, etc.

6. Contingut de l'activitat formativa del personal i membres de la corporació

Es consideren incloses, també, en l'àbast del contracte les accions formatives sobre Protecció de Dades Personals que no corresponguin al DPD, en concret, el contractista assumirà les següents tasques en matèria de formació dels diferents col·lectius de personal municipal i càrrec electes:



AJUNTAMENT D'ESPARREGUERA

1. Pels responsables dels Serveis/Departaments i càrrecs electes (amb una durada mínima de 4 hores anuals per tots els grups que es puguin formar): es portaran a terme les sessions de formació necessàries per traslladar el coneixement obtingut de l'anàlisi de la situació de l'ajuntament relatiu a l'objecte del contracte i donar-los les eines i coneixements necessàries per a la correcta aplicació de la normativa, en concret, inclourà com a mínim:
 - Els aspectes concrets i específics de LOPDGDD i ENS
 - Justificació normativa sobre els aspectes inclosos en la política de seguretat, en el document de seguretat i en el pla de millora de seguretat municipal.
 - Recomanacions i responsabilitats corresponents als Serveis/Departaments. Control accés a les dades personals i auditories
 - El rol del responsable del tractament (en coordinació amb el DPD)
2. Pels usuaris de l'eina de gestió documental es proposarà els sessions de formació necessària per a l'aplicació correcta de la LOPDGDD i ENS als documents administratius i el seu tractament, amb una durada mínima de 4 hores anuals per a tots els empleats municipals, en concret, inclourà com a mínim:
 - Principals mesures incloses en la política de seguretat, document de seguretat i en el pla de millora de la seguretat
 - Pautes generals per a l'aplicació de les mesures de seguretat
 - Control d'accessos a les dades personals
 - Recomanacions i responsabilitats dels usuaris
 - Obligacions de transparència, especialment de transparència activa, disposició de les dades a publicar i les autoritzacions corresponents.
3. Pel personal de Serveis Informàtics és proposarà els sessions de formació necessària per a l'aplicació correcta de l'ENS i l'ENI (amb una durada mínima de 4 hores anuals), en concret, inclourà com a mínim:
 - Document de seguretat i Esquema Nacional de Seguretat
 - Procediments de millora del sistema de gestió de la seguretat
 - Metodologies per a l'actualització de la documentació
 - Recomanacions i responsabilitats dels responsables de seguretat, dels administradors tècnics.

L'adjudicatari serà responsable d'impartir aquesta formació i de proporcionar tots els mitjans materials i personals necessaris per a la correcta realització de la formació, estant tots els treballs de formació inclosos en el preu de l'oferta.

L'Ajuntament facilitarà els espais per desenvolupar la formació o disposarà que aquesta es dugui a terme on-line.

7. Generalitats

No s'admetrà la presentació de variants o alternatives i no es valoraran aquelles ofertes que no presentin solucions a allò que estableix aquest plec. Les característiques tècniques i funcionals que es descriuen en aquest document tenen el caràcter de mínims.



**AJUNTAMENT
D'ESPARREGUERA**

8. Supervisió, control i seguiment

Es mantindran reunions formals de coordinació general amb el responsable municipal del contracte o Comissió de Seguretat i aquelles altres persones que es consideri adient, per a realitzar el seguiment del servei, amb una periodicitat trimestral.

Addicionalment, a petició de qualsevol de les parts, es podran organitzar reunions puntuals per abordar assumptes d'interès o de caràcter urgent.

9. Temps de resposta

Les consultes dels serveis es faran via correu electrònic, seran resoltes per l'empresa adjudicatària en un termini màxim de cinc (5) dies hàbils des de la data de la consulta efectuada.

Pel que fa al temps de resposta de les actuacions davant d'autoritats de control de protecció de dades, seran els establerts per les mateixes autoritats de control.

Per a la resta de serveis que suposen l'elaboració, revisió, manteniment i supervisió dels procediments, tasques i actuacions per adequar l'activitat municipal a la protecció de dades, es procedirà d'acord a allò que indiqui el responsable municipal del contracte o Comissió de Seguretat.

Esparreguera, a data de signatura electrònica.

Núria Mayoral Marimon
Serveis Jurídics, Contractació i Bon Govern

Miquel Campmany Segarra
Servei Sistemes Informació