

Número d'expedient: PACC2021000102

---

**PLEC TÈCNIC PER A LA CONTRACTACIÓ DEL SERVEI DE SUPORT EN  
MATÈRIA DE LA SEGURETAT DE LA INFORMACIÓ PER AL DESPLEGAMENT  
DEL REGLAMENT RGPD I DE LES MESURES PREVISTES AL PLA D'ADEQUACIÓ  
A L'ENS I ENI**

Procediment: obert simplificat

**ÍNDEX**

|      |                                                           |    |
|------|-----------------------------------------------------------|----|
| 1.   | INTRODUCCIÓ .....                                         | 1  |
| 2.   | OBJECTE DEL CONTRACTE .....                               | 4  |
| 3.   | ABAST DEL SERVEI .....                                    | 4  |
| 3.1. | REGLAMENT GENERAL DE PROTECCIÓ DE DADES .....             | 5  |
| 3.2. | ESQUEMA NACIONAL DE SEGURETAT I D'INTEROPERABILITAT ..... | 9  |
| 3.3. | CERTIFICACIÓ DE COMPLIMENT DE L'ENS .....                 | 12 |
| 4.   | DIMENSIONAMENT DELS SERVEIS .....                         | 12 |
| 5.   | HORARI DE PRESTACIÓ DELS SERVEIS .....                    | 13 |
| 6.   | ACORD DE NIVELL DE SERVEI .....                           | 13 |
| 7.   | SUPERVISIÓ, CONTROL I SEGUIMENT .....                     | 14 |

**1. INTRODUCCIÓ**

L'Ajuntament de Sant Feliu de Llobregat porta molts anys adaptant la seva organització als requeriments que successivament han anat imposant a les administracions públiques la normativa en matèria d'administració digital, de seguretat de la informació i de protecció de dades personals, per avançar en la progressiva actualització de les mesures tècnic-organitzatives aplicables als sistemes d'informació de l'Ajuntament, principalment recollides en l'actualitat en el Reglament (UE)/2016/679 Reglament General de Protecció de Dades i la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

A banda d'aquestes normatives essencials, en aquesta matèria el marc jurídic aplicable està integrat també per una tanda de lleis administratives encapçalades per la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, i la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic, que a la vegada han previst l'elaboració de dues normes que impacten directament en la necessitat d'adopció per part a les Administracions Públiques de mesures de protecció dels seus sistemes d'informació, dels serveis i les dades: els Esquemes Nacionals de Seguretat i d'Interoperabilitat. En concret l'ENS ha estat redefinit, per adaptar-lo a l'estat de la seguretat en l'actualitat, a través del Reial Decret 311/2022, de 3 de maig.

Altres normatives també reconeixen tot un conjunt de drets a la ciutadania i imposen obligacions a les Administracions públiques que impacten en la protecció de dades

personals, en matèries com la transparència, accés a la informació pública i bon govern (Llei estatal 19/2013 i Llei catalana 19/2014); de simplificació de l'activitat administrativa de la Generalitat i dels governs locals de Catalunya (Llei 16/2015); de reutilització de la informació (Llei 37/2007, modificada per Llei 18/2015); de contractació electrònica (Llei 9/2017); de l'activitat econòmica (Llei catalana 18/2020, de facilitació de l'activitat econòmica); entre d'altres.

Aquestes normatives incideixen en l'acompliment dels principis essencials de l'Administració Digital plasmats en els diferents plans, agendes i estratègies de tots els nivells d'administració territorial, i que partint de la UE tenen com a objectiu principal eliminar els obstacles digitals i evitar la fragmentació que es pot generar en el context de transformació digital de les administracions públiques.

En concret, la via per a la transformació digital que ha marcat en els darrers anys la UE abasta una sobirania digital oberta, de ple **respecte als drets fonamentals**, a l'Estat de Dret i la democràcia, la integració, l'accessibilitat, la igualtat, la sostenibilitat i els respecte als drets i aspiracions de totes les persones. En aquest sentit, la *Brúixola Digital 2030: l'enfoc d'Europa per al Decenni Digital* de 2021 es presenta la filosofia d'una Europa transformada digitalment en el respecte als valors europeus, on l'aspiració de la UE és ser digitalment sobirana en un món obert i interconnectat, amb ciutadans emancipats i empreses innovadores en una societat digital centrada en l'ésser humà, integradora, pròspera i sostenible, que ha estat seguida de la **Declaració europea sobre drets i principis digitals**, de 26 de gener de 2022 que vol avançar en la consecució del respecte als valors europeus en el marc de la transformació digital donant preeminència a les persones i de forma que la tecnologia digital beneficiï a la societat en el seu conjunt.

En aquest escenari, els nous reptes de l'enfortiment de les capacitats de prevenció, detecció i resposta als ciberatacs, potenciant i adoptant noves mesures per contribuir a la promoció d'un ciberespai segur i fiable. Per encarar aquest objectiu, l'evolució del marc de la ciberseguretat ha avançat cap a un escenari més integrador, coherent i inclusiu que permet desenvolupar serveis cada vegada més segurs i eficients i que ajuda a garantir la protecció de la informació del sector públic i dels serveis essencials, els seus sistemes i informacions, així com les xarxes que els suporten. Per tant, una visió integral de la seguretat requereix disposar de sistemes més integrats, orientats a l'alerta precoç, a la preparació de plans per a la gestió de les crisis i a la disposició d'instruments que ajudin a disminuir la vulnerabilitat dels sistemes i xarxes, que actuïn en el reforç de la seva resiliència.

El dret a la ciberseguretat es recull a la Carta espanyola de drets digitals, on s'estableix que qualsevol persona té dret a què els sistemes digitals d'informació que utilitzi en la seva activitat personal, laboral o social disposin de les mesures de seguretat adequades, i la necessitat que els poders públics promoguin la sensibilització i la formació en matèria de ciberseguretat de tota la societat, impulsant mecanismes de certificació.

Així, aquesta regulació es concreta en la necessitat que la ciberseguretat sigui abordada per l'administració des d'una perspectiva multidimensional, creant una cultura en aquesta matèria que es projecti tant en els processos ad intra de les organitzacions, com en aquells processos amb impacte en la ciutadania, democratitzant-ne el seu accés.

Tal com s'estableix a l'Estratègia Nacional de Ciberseguretat i a l'Estratègia de

Ciberseguretat de la Generalitat de Catalunya, la **seguretat del ciberespai** és una de les màximes preocupacions en el context actual de transformació digital. Per fer front a aquesta amenaça, l'Ajuntament seguirà avançant en el reforç de les capacitats per fer front a possibles ciberatacs i ús maliciós del ciberespai.

- **Ampliar i millorar les capacitats de detecció i anàlisi de les ciberamenaces** a fi d'identificar procediments
- **Potenciar la col·laboració amb altres organismes** en la lluita contra els ciberatacs.
- **Desenvolupar i actualitzar les normes, procediments i instruccions** de resposta enfront a incidents de seguretat o possibles casuístiques.
- **Establir un conjunt de mètriques** de les principals variables de ciberseguretat per tal de determinar el nivell de seguretat i la seva evolució.
- **Realitzar avaluacions periòdiques** en matèria de ciberseguretat.

Finalment, senyalar que a l'Agenda Digital de l'Ajuntament de Sant Feliu s'identifica, dins l'eix 2 – Infraestructures digitals i serveis TIC, l'objectiu estratègic “Crear les condicions necessàries de ciberseguretat” en el qual s'identifiquen quatre línies d'actuació.

Aquest marc ha de guiar els responsables de les polítiques per a una concepció concreta de la transformació digital que ha **de promoure i protegir els valors en l'entorn digital: la intimitat, el control individual de les dades**, la igualtat d'accés als serveis, la participació en l'espai públic **o la llibertat d'elecció en la interacció amb els algorismes i els sistemes d'intel·ligència artificial**, així com en un entorn digital equitatiu que requereix d'un augment de la seguretat i la protecció en l'entorn digital.

En aquest sentit, la vigilància i el compliment de la normativa en protecció de dades personals que actualment es concreta en el Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016, Reglament General Europeu de Dades (RGPD) i la Llei orgànica 3/2018 (LOPDGDD), i la protecció dels seus sistemes, serveis, i dades, és per a l'Ajuntament de Sant Feliu de Llobregat una peça clau i essencial sobre la qual pivoten la resta d'instruments i eines necessàries per a la transformació digital de la seva organització i del municipi.

Així mateix, l'Ajuntament, igual que la resta d'Administracions públiques, ha de treballar sota el marc comú de seguretat fixat en el Reial Decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat (ENS) per a la protecció dels sistemes d'informació, que requereix com a condició obligatòria que la corporació disposi de sistemes segurs per a l'exercici de les seves competències i inclogui la gestió de riscos en tots els seus processos de negoci, així com en matèria de Ciberseguretat, incorporar les disposicions que s'estableixin tant des del Instituto Nacional de Ciberseguridad de España (INCIBE) com des de l'Agència de Ciberseguretat de Catalunya, així com amb les directrius i polítiques promogudes en

el marc de la Unió Europea.

## **2. OBJECTE DEL CONTRACTE**

L'objecte d'aquest contracte és la prestació dels següents serveis de suport:

- Suport al desplegament de les mesures previstes en el marc del Reglament (UE) 2016/679 RGPD i de la LO 3/2018 LOPDGDD, i a les tasques que ha de realitzar el DPD (Delegat/da de Protecció de Dades) en el marc de l'Organització de la Seguretat de l'Ajuntament de Sant Feliu de Llobregat
- Suport a l'actualització i desplegament de les mesures previstes en el nou RD 311/2022, de 3 de maig ENS i altres disposicions en matèria de ciberseguretat, així com, les accions derivades del Pla d'Adequació a l'Esquema Nacional de Seguretat i l'Esquema Nacional d'Interoperabilitat aprovat per l'Ajuntament de Sant Feliu de Llobregat.
- Acompanyament integral per a la certificació de compliment de l'ENS.

## **3. ABAST DEL SERVEI**

Els serveis objecte d'aquesta licitació comprenen tres línies de treball marcadament diferenciades de serveis d'assistència tècnica i suport:

- Suport al desplegament de les mesures previstes en el marc del Reglament General de Protecció de Dades, Reglament (UE) 2016/679 RGPD i de la LO 3/2018 LOPDGDD, i a les tasques que ha de realitzar el Delegat de Protecció de Dades, en el marc de l'Organització de la Seguretat de l'Ajuntament de Sant Feliu de Llobregat, que es detallen en el punt 3.1, així com l'anàlisi i la supervisió del compliment de la normativa RGPD en el marc contractual de l'Ajuntament.
- Suport a l'actualització i desplegament de les mesures previstes en el nou RD 311/2022, de 3 de maig ENS, així com la revisió, actualització i completesa de les actuacions desenvolupades en el marc del Pla d'Adequació a l'Esquema Nacional de Seguretat i l'Esquema Nacional d'Interoperabilitat aprovat per l'Ajuntament de Sant Feliu de Llobregat, que es detallen en el punt 3.2, i el seguiment i actualització dels plans de contingència previstos a la normativa d'Administració digital.

S'inclou també en aquest apartat el suport per a l'anàlisi, desenvolupament i

implementació d'un Pla de mesures de prevenció i correcció de vulnerabilitats per a la protecció física dels actius i els procediments de control davant d'amenaques que comprometin la continuïtat dels serveis causades per desastres naturals (incendis, inundacions, tempestes...), accidents, errors humans, etc. Aquestes mesures han d'estar alineades amb les disposicions en matèria de ciberseguretat que s'estableixin tant des del Instituto Nacional de Ciberseguridad de España (INCIBE) com des de l'Agència de Ciberseguretat de Catalunya, així com amb les directrius i polítiques promogudes en el marc de la Unió Europea.

- Acompanyament integral per a la certificació de compliment de l'ENS, donant suport al procés de tramitació de la sol·licitud fins l'obtenció de la mateixa.

### **3.1. REGLAMENT GENERAL DE PROTECCIÓ DE DADES**

Les funcions, activitats i tasques a desenvolupar en el marc de la protecció de dades personals són les següents:

1. Assessorar, informar i supervisar en el compliment de la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD) i al Reglament (UE)2016/679 (RGPD) i altres disposicions de protecció de dades personals a l'Ajuntament de Sant Feliu de Llobregat d'acord amb les funcions indicades a l'article 39 del RGPD i les recomanacions de les autoritats competents, inclòs l'assessorament al DPD de l'Ajuntament de Sant Feliu de Llobregat.
2. Lliurar informació periòdica sobre l'existència i/o modificació de normativa sectorial que pugui determinar condicions de tractament específiques diferents de les establertes per la normativa general de protecció de dades, almenys les relatives a:
  - Esquema Nacional de Seguretat
  - Llei d'infraestructures crítiques
  - Prestadors de serveis digitals
3. Donar compliment de la normativa en matèria de protecció de dades personals en el marc dels processos de contractació de l'Ajuntament.
4. Cooperar amb l'autoritat de control i suport en els comunicacions de bretxes de dades personals accidentals o il·lícites de l'article 33 RGPD.

5. Respecte les Avaluacions d'Impacte:

- Assessorar en matèria d'Avaluacions d'Impacte relativa a la protecció de dades personals.
- Determinar la metodologia a utilitzar i suport en l'elaboració d'anàlisis d'impacte.
- Dur a terme les avaluacions d'impacte de tractament de dades responsabilitat de l'Ajuntament de Sant Feliu de Llobregat i les seves entitats com a Responsable de Tractament o en qualitat d'Encarregat de Tractament. S'inclourà un mínim de 10 avaluacions d'impacte anuals de mitjana, independentment de les que es puguin dur a terme de manera contínua en els processos de control i revisió dels tractaments actuals.
- Determinar les salvaguardes jurídiques, tècniques i organitzatives segons els resultats de l'anàlisi d'impacte.
- Proposta d'implantació de les mesures de seguretat adequades als riscos i la naturalesa dels tractaments.
- Si la implantació de les mesures adequades s'ha realitzat correctament o no i si les conclusions són conformes amb el RGPD i la LOPDGDD.

6. Mantenir i desplegar el Pla de contingència

7. Revisar, actualitzar i gestionar contínuament el Registre d'Activitat de Tractament de l'Ajuntament, que inclourà:

- Compliment dels principis de tractament com els de limitació de finalitat, minimització o exactitud de les dades.
- Valoració de la compatibilitat de les finalitats diferents de les que van originar la recollida inicial de les dades.
- Identificar els diferents tipus de dades personals recollides i tractaments per l'Ajuntament de Sant Feliu de Llobregat i els seus organismes autònoms i vinculats a l'exercici de les seves competències.
- Analitzar les bases jurídiques dels tractaments.
- Recollir la informació definida al RGPD i addicionalment: Identificar els mitjans concrets de recollida o procedència de les dades (formularis, comunicació de dades, etc.), identificar els sistemes concrets d'informació utilitzats per al tractament de les dades.
- Suport en el procés d'automatització del RAT.

En l'actualitat, el nombre de tractaments identificats com a Responsable de Tractament són 436.

8. Gestionar l'exercici de drets per part dels interessats, que inclourà:
  - Valoració de les sol·licituds d'exercici de drets amb el suport dels responsables dels àmbits corresponents.
  - Coordinació de les tasques necessàries per a l'execució dels drets, en cas que siguin afirmativa l'anàlisi.
  - Resolució i proposta de resposta als interessats que exerceixin els seus drets davant de la Corporació.
  - Elaboració d'informe sobre l'exercici realitzat, si és requerit per l'Ajuntament.
  - Revisió dels mecanismes de recepció, coordinació i gestió de les sol·licituds d'exercici de drets per part dels interessats.
9. Definir, revisar i/o elaborar els procediments, els protocols i les instruccions aplicables per a la gestió de dades personals: procediment de gestió i comunicació de violació de seguretat de dades, procediment de gestió d'exercici de drets, definició dels controls regulars, suport en el desplegament de la política de rols i suport en el desplegament de les mesures de seguretat establertes en el Model de Governança de les dades de Sant Feliu.
10. Col·laborar en l'elaboració de la documentació de diferents àmbits que afecti l'àmbit de la protecció de dades i que derivi de l'assessorament efectuat pel delegat de protecció de dades.
11. Adequar-se permanentment a la normativa interna, dels protocols de treball i models de documents als criteris i requeriments de la legislació en matèria de protecció de dades.
12. Dissenyar i implantar mesures de compliment del dret d'informació a les persones interessades, amb la revisió individualitzada de documents, formularis, contractes, polítiques de privacitat, etc..
13. Impartir formació estratègica. Formació, tant des del vessant teòric com a aplicació pràctica en matèria de protecció de dades segons la realitat concreta de cada col·lectiu o àmbit i les tasques i obligacions del personal. Es duran a

terme un mínim de 6 sessions de formació de 2 hores cadascuna, a personal tècnic i administratiu.

14. Assistir a les reunions de la Comissió de Seguretat semestral així com a les convocatòries realitzades mensualment per l'Ajuntament i/o la Subcomissió de Seguretat, quan s'escaigui.

15. Donar suport online a qüestions, consultes, revisió de documentació, etc., amb un temps de resposta màxim de 3 dies laborables. Es preveu una mitjana de 100 consultes anuals.

16. Realitzar controls regulars i auditories de compliment del RGPD i LOPDGDD

- De forma regular es realitzaran controls i verificacions sobre determinats àmbits segons es determini a la Comissió de Seguretat de l'Ajuntament, com ara sobre el compliment dels avisos legals i llegendes informatives als portals web, valoració del nivell d'aplicació de les mesures de seguretat en funció de l'Avaluació d'Impacte del tractament o els requisits de l'RGPD, nivell de coneixement del personal, etc.. Els informes amb els resultats de l'avaluació d'aquests controls seran presentats a la Comissió de Seguretat.
- Realització d'auditoria de compliment de la legislació vigent en matèria de protecció de dades personals. A l'inici del contracte, s'hauran de realitzar una auditoria de compliment de l'RGPD i Llei Orgànica de Protecció de Dades Personals i Garantia de Drets Digitals en el seus àmbits jurídics, tècnics i organitzatius.

L'adjudicatari haurà de lliurar, com a mínim, la següent documentació:

- Informe d'auditoria d'acord amb el que estableix la normativa, que recollirà els resultats de l'auditoria.
- Descripció de mesures correctores o complementàries necessàries i pla d'acció.
- Resum executiu amb els resultats i les conclusions de l'auditoria.

17. Portar a terme sessions de formació i/o reunions amb els responsables d'àrea de l'Ajuntament per revisar principis i procediments del RGPD, especialment envers l'anàlisi de riscos previ de qualsevol nou servei per determinar l'impacte sobre el tractament de dades, contemplant entre altres aspectes els següents:

- Necessitat d'una Avaluació d'Impacte
- Determinació de mesures tècniques

- Regulació de relació contractual
18. Definir un Pla Estratègic de Formació, començant amb correus electrònics amb píndola informativa recordatori de principis RGPD.
  19. Plantejar controls i auditories regulars, per validar el nivell d'implantació dels procediments RGPD, un cop reforçat el sistema.
  20. Tractar la protecció de dades en la reglamentació del teletreball.

### **3.2. ESQUEMA NACIONAL DE SEGURETAT I D'INTEROPERABILITAT**

Les funcions, activitats i tasques a desenvolupar en el marc de la seguretat dels sistemes d'informació d'acord amb l'ENS i l'ENI són les següents:

1. Esquema Nacional de Seguretat (ENS)
  - Revisió actualització de la documentació en matèria de seguretat de la informació:
    - Política de seguretat de la informació, marc organitzatiu i operacional  
Procediments TIC segons nou ENS
    - Codi de bones pràctiques (normes d'usuari)
  - Revisar la categorització dels sistemes d'informació atenent a la valoració de la informació i dels serveis prestats, si s'escau.
  - Realitzar l'anàlisi de riscos (tasca anual) associats a cada tractament existent proposant mesures de seguretat concretes establertes a l'Annex II de l'ENS, per minimitzar-los o eliminar-los. De tots els procediments electrònics i sistemes informàtics que s'incorporin.
  - Assessorament, acompanyament i supervisió en la implantació i seguiment de procediments i mesures de seguretat aplicables i la seva classificació referida al grau d'implementació de cadascuna de les mesures de seguretat.
  - Revisar i actualitzar, si s'escau i aprovar la Declaració d'aplicabilitat de las mesures de seguretat previstes en l'Annex II del ENS.
  - Suport i validació en operació i monitorització de las mesures de seguretat per a una gestió continuada de la seguretat.

- Actualitzar el pla d'adequació per a la millora de la seguretat, sobre la base de les insuficiències detectades, incloent terminis estimats d'execució.
- Suport en l'elaboració de documentació per presentar a la Comissió de Seguretat.

## 2. Avaluació i preparació per la certificació de compliment de l'ENS

- Auditoria que s'haurà de realitzar conjuntament amb la pròpia de la normativa de dades personals. Caldrà una auditoria a l'inici del contracte.
- Auditoria biennal: Enfocament de la supervisió i assessorament basat en el risc: assessorar, assumir la realització i supervisió d'auditories d'interne o coordinació d'auditories externes.
- Revisió dels requeriments i preparació de la documentació per a la certificació de compliment de l'ENS.

## 3. Esquema Nacional d'Interoperabilitat (ENI)

Tasques de suport i assessorament per al compliment de les obligacions que corresponen a l'Ajuntament recollides al Reial Decret 4/2010, de 8 de gener, pel que es regula l'Esquema Nacional d'Interoperabilitat, en l'àmbit de l'administració electrònica i les Normes Tècniques d'Interoperabilitat que el desenvolupen, que amb caràcter enunciatiu i no limitatiu són essencialment les següents:

- Auditoria i diagnosi del compliment de mesures de l'ENI, amb una periodicitat mínima biennal
- Suport, assessorament i manteniment continu en la implantació i compliment de l'ENI
  - Interoperabilitat organitzativa: publicació de serveis a través de la Xarxa de comunicacions de les Administracions Públiques, inventaris de la informació administrativa, etc.
  - Interoperabilitat semàntica: Publicació i aplicació dels models de dades d'intercanvi, identificació i publicació dels models de dades, etc.
  - Interoperabilitat tècnica: ús estàndards oberts, etc.
  - Utilització d'infraestructures i serveis comuns i eines informàtiques genèriques
  - Utilització de la xarxa de comunicacions de les Administracions Públiques
  - Reutilització i transferència tecnològica: Condicions de llicenciament de

les aplicacions, directoris d'aplicacions reutilitzables, etc.

- Normes de conformitat: establiment de polítiques de control, etc.
- Revisió i modificació dels Procediments tècnics i de l'aplicació dels estàndards d'interoperabilitat per garantir el compliment de la normativa vigent
- Anàlisi i assessorament de compliment dels nous procediments/documents electrònics i sistemes informàtics que s'incorporin a l'Ajuntament, així com els ja presents a l'actualitat
- Suport online sobre aspectes i dubtes en l'aplicació de l'ENI: resolució de dubtes i consultes derivades de les tasques habituals de l'Ajuntament en els procediments i mesures establertes
- Servei de suport i manteniment continuat del sistema fins a la finalització del servei

Aquestes tasques es desenvoluparan en coordinació amb el DPD i el Departament de Sistemes d'Informació.

#### 4. Pla de contingència i continuïtat de negoci

- Definició dels interlocutors i recursos organitzatius en situació de crisi
- Revisió i aprovació de procediments del Pla de Contingències
- Mantenir i desenvolupar el pla de contingència.
- Inclusió i relació amb el Pla de protecció civil municipal (Document únic de protecció civil municipal - DUPROCIM)
- Garantir la privacitat i intimitat en els documents eliminant les persones responsables i el seu equip.
- Revisió del procediments TIC i AOC.
- Validació dels recursos de contingència.
- Determinació de la informació interna de prioritització dels serveis i recursos mínims de cada servei en funció de la seva sensibilitat i criticitat.
- Definició dels interlocutors i recursos organitzatius en situació de crisi.
- Revisió i aprovació de procediments Pla de Contingències.

5. Participació en la comissió de seguretat: proposta de tasques de recolzament necessàries per administrar, gestionar i controlar la seguretat de la informació i la protecció de dades a l'Ajuntament.
6. Suport online sobre aspectes de l'aplicació de l'ENS: resolució de dubtes i consultes derivades de les tasques habituals de l'Ajuntament en els procediments i mesures establertes.
7. Formació del personal.

### 3.3. CERTIFICACIÓ DE COMPLIMENT DE L'ENS

Es portarà a terme un acompanyament integral per la certificació de compliment de l'ENS, portant a terme totes les activitats que siguin necessàries fins l'obtenció de la certificació, entre les quals tindrem les següents:

- Assessorament tècnic i jurídic
- Preparació de la documentació
- Tramitació de la sol·licitud de certificació amb una Entitat de Certificació autoritzada pel CCN (Centro Criptológico Nacional)
- Suport en tot el procés de tramitació

Els licitadors inclouran a la seva proposta totes les despeses derivades de l'obtenció de la certificació de compliment de l'ENS, incloent el cost del servei de l'Entitat de Certificació autoritzada que emeti el certificat.

## 4. DIMENSIONAMENT DELS SERVEIS

La dedicació global mínima exigida per atendre els serveis demanats s'estima en 2100 hores, repartides al llarg de la durada del contracte entre els membres de l'equip de treball assignat, segons el següent quadre:

| Any   | 2023 | 2024 | 2025 | 2026 | 2027 |
|-------|------|------|------|------|------|
| Hores | 140  | 544  | 500  | 500  | 416  |

Aquest repartiment s'ha d'entendre com temptatiu, de manera que la dedicació efectiva pot variar en funció de les necessitats de cada moment, sempre mantenint l'esforç global del contracte.

La distribució de la dedicació entre els membres de l'equip de treball adscrit al

contracte serà la necessària atenent les funcions que realitzi cadascú. En el cas d'adscriure al contracte més de dues persones, la dedicació dels dos perfils professionals mínims exigits als requeriments de solvència tècnica i professional, recollits al plec de clàusules administratives particulars, haurà de ser com a mínim el 90% de la dedicació global exigida per al contracte.

Pel control de l'esforç dels serveis prestats, l'adjudicatari portarà un registre de totes les activitats realitzades, la seva descripció, i detall de la dedicació en hores. Aquest registre es compartirà amb el responsable del contracte de l'Ajuntament, que l'haurà de validar.

La dedicació en hores imputada en el registre correspondrà a les hores efectives dedicades a les activitats que formen part de l'abast dels serveis demanats.

## 5. HORARI DE PRESTACIÓ DELS SERVEIS

L'horari mínim per la prestació dels serveis serà el següent:

| Horari                                            |
|---------------------------------------------------|
| De 9:00 a 17:00 de dilluns a divendres laborables |

Els dies laborables seran els determinats pels calendaris oficials definits per la Generalitat de Catalunya i per la ciutat de Sant Feliu de Llobregat.

## 6. ACORD DE NIVELL DE SERVEI

El paràmetre que es tindrà en compte en l'Acord de Nivell de Servei (ANS) per la mesura de la qualitat dels serveis prestats serà el **temps de resposta** davant les peticions de servei i consultes, pel qual es defineixen tres nivells de prioritat amb els següents objectius de compliment mínims:

| Prioritat | Temps de resposta |          |
|-----------|-------------------|----------|
|           | Condició          | Objectiu |
| Alta      | <= 2h             | 90%      |
|           | <= 4h             | 100%     |
| Mitja     | <= 4h             | 90%      |
|           | <= 8h             | 100%     |
| Baixa     | <= 16h            | 80%      |

Es defineix com a **temps de resposta** el temps transcorregut des de la notificació

de la petició de servei o consulta pels canals establerts, fins que el prestador del servei inicia les accions específiques per atendre el cas, incloent l'anàlisi i avaluació preliminar del mateix i la comunicació a l'interessat d'un compromís de temps de resolució.

Els temps transcorreguts es consideren dins la finestra horària de servei, per tant, per la seva mesura es comptabilitzarà només el temps transcorregut dins la franja horària de prestació de servei.

La prioritat dels casos la determinarà l'Ajuntament atenent criteris de criticitat, urgència i impacte en l'organització i en els serveis oferts a la ciutadania.

## **7. SUPERVISIÓ, CONTROL I SEGUIMENT**

Es mantindran reunions periòdiques de coordinació general amb la Subcomissió de Seguretat de l'Ajuntament per realitzar el seguiment de la prestació del servei.

La finalitat darrera de les reunions és la comprovació del compliment en la prestació dels serveis mitjançant una comunicació periòdica i formal entre els interlocutors de l'Ajuntament i de l'empresa adjudicatària.

Adicionalment, a petició de qualsevol de les parts, es podran organitzar reunions puntuals per abordar assumptes d'interès que hagin de ser tractats apart o abans de la propera reunió periòdica.

Manuel González Maya  
Cap del Departament de Sistemes  
d'Informació

[Firma01-01]

Sandra González Aguilera  
Tècnica d'Administració Digital

[Firma02-01]

