



ANNEX 1: SERVEI DE SIGNATURA BIOMÈTRICA, SIGNATURA AMB DOBLE FACTOR I SIGNATURA ELECTRÒNICA AL NÚVOL

1. INTRODUCCIÓ

La Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de las Administracions Públiques (LPAC), regula les relacions externes entre l'Administració i la ciutadania i té com a objectiu la implantació d'una Administració totalment electrònica, millorant l'agilitat dels procediments administratius i reduint els temps de tramitació.

Encara són molts els tràmits i els procediments que es desenvolupen de manera presencial entre l'administració i els interessats.

L'article 10 de la LPAC, estableix que els interessats podran signar a través de qualsevol mitjà que permeti acreditar l'autenticitat de l'expressió de la seva voluntat i el consentiment, així com la integritat i la inalterabilitat del document, i que aquest mateix article atorga potestat a les Administracions Públiques per determinar quin sistema admet per a realitzar determinats tràmits o procediments del seu àmbit de competència.

L'article 12 d'aquest mateix text legal estableix, en el seu apartat primer, que les administracions públiques hauran de garantir que els interessats podran relacionar-se amb l'administració a través de mitjans electrònics, pel que es posarà a la seva disposició els canals d'accés que siguin necessaris, així com els sistemes i aplicacions que en cada cas es determinin i que, en el seu apartat segon, determina que les administracions públiques assistiran en l'ús de mitjans electrònics als interessats, en el referent a la identificació i signatura electrònica i presentació de sol·licituds a través del registre electrònic general.

Així mateix, l'article 70 de la LPAC estableix que els expedients administratius han de tenir format electrònic i determina la interoperabilitat entre les administracions Públiques, de conformitat amb l'Esquema Nacional d'Interoperabilitat i les Normes Tècniques d'Interoperabilitat.

Que l'admissió d'un sistema de signatura electrònica manuscrita, a través de dispositius de captura biomètrica de la signatura dels interessats conjuntament amb la signatura electrònica dels documents, és perfectament admissible, sempre



que aquest sistema reuneixi els requisits establerts a l'article 10 i 70 de la LPAC i que les dades personals que resultin de la utilització del sistema de signatura, donin compliment i s'ajustin a allò disposat al Reglament (UE) 2016/679, General de Protecció de Dades RPGD i a la Llei Orgànica 3/2018, de Protecció de Dades Personals i Garantia dels Drets Digitals LOPDGDD.

Que per tal de facilitar la presentació electrònica als interessats que ho facin presencialment sense mitjans electrònics, es considera tècnicament que la forma més eficient, tant pel ciutadà com per la corporació municipal, és disposar d'un sistema de signatura electrònica manuscrita que inclou la captura biomètrica de la signatura dels interessats, a través de dispositius especialitzats així com la signatura electrònica automatitzada de tal manera que, amb la combinació de les dues tecnologies, es garanteix l'autenticitat de l'expressió de la voluntat i consentiment de l'interessat, la integritat i autenticitat del document signat i la perdurabilitat en el temps.

Que d'acord amb la Llei Orgànica 3/2018, de Protecció de Dades Personals i Garantia dels Drets Digitals, aquesta solució ha de garantir la confidencialitat de les dades biomètriques de la signatura dels interessats.

Que de conformitat amb l'article 70 de la LPAC, es garantirà la interoperabilitat amb les administracions Públiques, de conformitat amb l'Esquema Nacional d'Interoperabilitat i les Normes Tècniques d'Interoperabilitat vigents en cada moment, en la remissió de documents electrònics generats utilitzant el sistema de signatura biomètrica.

2. OBJECTE DEL CONTRACTE

L'objecte és la contractació de serveis al núvol següents:

- Signatura biomètrica que permeti la signatura electrònica manuscrita
- Signatura amb doble factor que permeti la signatura electrònica de documents mitjançant correu electrònic i un segon factor amb una clau d'un sol ús al mòbil
- Signatura al núvol que permeti la signatura electrònica amb els certificats digitals custodiats en un servidor HSM

3. REQUISITS TÈCNICS



Els serveis han de complir els següents requisits tècnics:

3.1. SIGNATURA BIOMÈTRICA:

S'utilitzarà principalment en les oficines i espais d'atenció ciutadana així com en dispositius d'actuació mòbil del personal municipal com potser inspeccions, assistència domiciliària o actes de la Guàrdia Urbana. Caldrà que compleixi els següents requisits:

- La signatura dels documents s'ha de realitzar en dispositius tàctils dedicats, igual que es realitzaria sobre un paper, proveïts per la corporació municipal. Almenys haurà de suportar els següents dispositius biomètrics que actualment es disposen: HUAWEI MEDIAPAD M2 10", Samsung Galaxy Tab A S6Lite, Samsung Tab Active3 i MICROSOFT SURFACE PRO 8. El contractista restarà obligat a actualitzar aquesta llista anualment disponible per mitjans electrònics.
- Ha de permetre l'ús dels dispositius assignats a diferents subscripcions o aplicacions municipals diferenciant entitats municipals per facilitar la seva gestió i seguiment.
- El contractista actuarà com a tercer de confiança, amb capacitat tecnològica suficient per a la captura de dades biomètriques de la signatura del document de la persona per garantir la seva autenticitat sense cap tipus de manipulació.
- En el cas de més d'una persona signant, el servei enviarà el document a signar progressivament a tots les persones signants fins que es realitzin totes les signatures biomètriques. Es podrà escollir la ubicació on es visualitzi la signatura electrònica.
- Garantir que el document que es mostra al dispositiu coincideix amb el document que se signa (WYSIWYS -What you see is what you sign).
- Realitzar una signatura electrònica avançada amb segell de temps sobre el document incloent les metadades dotant així d'integritat al document signat.
- Les dades biomètriques no podran ser accessibles en cap cas ni per la corporació municipal ni per cap tercer per garantir la seva confidencialitat. Aquestes seran encriptades mitjançant clau que estarà dipositada davant notaria o sistema similar de tal manera que en cas de litigi o reclamació de l'autenticitat de la signatura biomètrica, serà necessari un tercer de confiança. D'aquesta manera, es garanteix la integritat i perdurabilitat de la signatura biomètrica inclús si el contractista no continua el servei. La informació de la notaria que custòdia la clau o sistema similar ha de ser informació pública que posseeix el document signat.



- S'ha de disposar d'un component per Microsoft Word 2010 o superior, per Libreoffice versió 7 d'una aplicació web responsiva i d'una impressora virtual per Windows 10 o superior per enviar i rebre documents a signar.
- La signatura electrònica automatitzada haurà de ser PadES B-LT de llarga durada per documents PDF.
- Les dades biomètriques s'emmagatzemaran dins el mateix document en base a l'estàndard ISO/IEC 19794-7 per garantir la interoperabilitat i el seu peritatge posterior si s'escau.
- La volumetria estimada de dispositius municipals a utilitzar signatura biomètrica serà fins a un màxim de 60 sense limitació del nombre de signatures de documents. Actualment es disposa de 25 dispositius i es fan 14.000 signatures biomètriques anuals però l'objectiu és anar proveint progressivament més dispositius per noves necessitats previstes durant la durada del contracte fins al màxim estimat.
- El licitador haurà de presentar un dictamen jurídic del compliment de la normativa en matèria de validesa de la signatura manuscrita recollida per captura de dades biomètriques, signatura electrònica avançada, normativa d'administració electrònica i interoperabilitat, normativa de protecció de dades de caràcter personal i garantia de confidencialitat de les dades biomètriques.

3.2. SIGNATURA AMB DOBLE FACTOR:

S'utilitzarà per recollir la voluntat expressa de la persona interessada de forma remota electrònicament com la confirmació d'una sol·licitud proposada a instància de part de la corporació municipal, la recollida d'un consentiment o altres documents o sol·licituds on la verificació de la identitat s'ha realitzat amb anterioritat per la corporació municipal sempre i quan, es disposi de les dades de correu electrònic i mòbil de la persona on ha expressat la seva voluntat que aquestes siguin usades com a mitjà de comunicació. Caldrà que compleixi els següents requisits:

- El contractista, com a tercer de confiança és qui recopila totes les evidències que s'han produït durant el procés de la signatura certificant la generació de la prova.
- La robustesa de la signatura dependrà de la quantitat d'evidències recollides.
- El sistema es considera signatura electrònica avançada basada en la signatura d'un document enviat a una adreça de correu electrònic, més la generació posterior d'un codi segur d'un sol ús (OTP) enviat per SMS al mòbil del destinatari que reconeix està sota el seu control exclusiu, més la grafia de la signatura.



- Es disposarà d'una aplicació web responsiva per poder enviar i rebre els documents per signar per aquest servei.
- El procés ha de ser el següent o equivalent:
 - > La persona rep un enllaç per correu electrònic que li dóna accés a una web de signatura. El format del correu ha de poder personalitzar-se en part tant en el contingut com en el disseny.
 - > Des de la web responsiva adaptada a qualsevol dispositiu, la persona pot revisar el document a signar.
 - > Quan la persona decideix signar el document, rep un OTP (codi d'un sol ús) per SMS al seu mòbil amb el què signa el document.
 - > La persona grafia la signatura al dispositiu.
 - > Es crea un OTC-One Time Certificate a nom i DNI del signant per vincular la signatura i la persona, que s'usa per signar electrònicament amb el corresponent segell de temps qualificat
 - > El servei recollirà totes les evidències del procés i compon el certificat del procés de signatura, i el remet a l'emissor.
- Les principals evidències requerides que identifiquen la persona per vincular signatura i signant són:
 - > Nom i DNI del signant
 - > Correu electrònic sota control de la persona destinatària
 - > Número de mòbil de la persona destinatària on s'envia un OTP via SMS
 - > Grafia manuscrita de la signatura
- Es recullen evidències d'entorn i del context que són registrades per crear un informe de la transacció de signatura certificada pel tercer de confiança:
 - Hash del document IP, navegador, sistema operatiu
 - Si el signant ho accepta, geolocalització del moment de signatura.
 - Cada acció realitzada i temps exacte en què es va realitzar.
- La volumetria anual de signatures d'aquest tipus és actualment de 2.000

3.3. SIGNATURA ELECTRÒNICA AL NÚVOL:

- Signatura electrònica avançada o qualificada utilitzant certificats digitals qualificats emesos al personal municipal i emmagatzemats en un entorn segur.
- Disposar d'un servei d'HSM securitzat per tal de poder allotjar els certificats i on es custodiï per part del contractista les claus de signatura del personal municipal.
- Proporcionar un portasignatures web responsiu que permeti l'accés del personal municipal a un entorn on poder enviar, rebre i signar els documents i consultar l'estat de les signatures.



- Ha de poder permetre definir el temps màxim per la signatura del document.
- Disposar d'un mecanisme d'accés mitjançant una cartera d'identitat que faciliti l'accés al portasignatures sense haver de gestionar contrasenyes. D'aquesta manera, es permetrà controlar l'accés al portasignatures de signatures centralitzades mitjançant usuari/contrasenya o amb seguretat avançada basada en un doble factor d'autenticació (2FA) utilitzant una app criptogràfica (Wallet per IOs i android en les seves últimes dos versions vigents) com a disparador i gestor de l'accés, sota el control exclusiu de cada persona usuària. Es requereix compliment amb el model eIDAS2, que disposi del Conformance Test de EBSI.

3.4. REQUISITS COMUNS:

- Cal disposar d'un panell integral sense limitació d'usuaris on permeti saber l'ús i estat de tots els serveis de signatura. En el cas de signatura biomètrica les signatures realitzades i ús dels diferents dispositius i en el cas de signatura amb doble factor i signatura electrònica, l'ús i el volum de signatures disponibles i utilitzades permeten la seva consulta per diferents filtres com entre dates, dispositius, persones, ... Aquest panell haurà de permetre disposar d'usuaris per la propia gestió de cada entitat municipal i disposar d'un superadmin per poder supervisar tots els serveis de totes les entitats municipals.
- Disposar d'una completa API que permeti totes les funcionalitats disponibles en tots els serveis per servei web REST en format JSON per canal segur HTTPS SSL.
- Permetre ja sigui enviant-la per l'aplicació corresponent o per API, de la signatura de qualsevol dels tipus de serveis prestats per diferents persones sense importar l'ordre o amb un ordre definit, d'un document electrònic ja sigui per signatura biomètrica i/o signatura amb doble factor i/o signatura electrònica al núvol.
- Disposar d'un entorn de test per fer proves d'integració i validació funcional i un de productiu. L'entorn de test no consumirà cap llicència d'ús de dispositius tàctils i només es podrà aplicar la restricció del servei per llicències d'ús en l'entorn productiu.
- Formacions o webinars quan sigui necessari.
- Conforme l'article 21 del Reglament (UE) Núm. 910/2014, el licitador ha d'acreditar ésser inclòs a la llista de confiança de prestadors qualificats de serveis electrònics de confiança estatal.
- Tots els serveis han de funcionar les 24 hores del dia i els 365 dies de l'any en el núvol.



4. INTEGRACIONS, FORMACIONS I POSADA EN MARXA DEL SERVEI

Es requereix que tots els serveis indicats estiguin disponibles en les següents aplicacions corporatives municipals:

- Registre d'entrada T-Systems mitjançant integració API per part dels tècnics municipals
- Expedients municipals propi mitjançant integració API per part dels tècnics municipals
- Inspeccions de salut de salut pública propi mitjançant integració API per part dels tècnics municipals
- Gestió de Recursos Humans «Epsilon» de Grupo Castilla
- Gestió tributària «SIT» de GTT
- Gestió policial «DRAG» de DRAGCLIC
- SAP (requereix addicionalment un integrador especialitzat)
- Navision (requereix addicionalment un integrador especialitzat)

Es requereix seguir disposant de la possibilitat de poder enviar un document a signar amb qualsevol dels tipus de serveis sota demanda i de manera independent a la integració demanada, mitjançant una aplicació web responsiva.

L'API disponible haurà de permetre qualsevol funcionalitat que disposa també el servei a través d'aplicacions d'usuari. Caldrà adjuntar la documentació de la API disponible.

Per tal de posar en marxa el servei, caldrà una formació prèvia de totes les funcionalitats de la plataforma així com de l'API als tècnics municipals designats i per totes les entitats municipals que participen.

També caldrà disposar de les integracions anteriorment indicades en el moment que el licitador presenti oferta.

Se signarà una acta d'inici de servei, deixant constància del compliment de requisits a partir de la qual comptarà com inici prestació del servei i de facturació.

5. SERVEI DE SUPORT, MANTENIMENT I ACTUALITZACIÓ



El licitador haurà de presentar una proposta de servei tècnic de suport, manteniment i actualització del servei i programari objecte del contracte. Dins aquesta proposta haurà d'indicar les característiques i la certificació del suport tècnic.

El suport i manteniment haurà d'estar garantit durant la durada del contracte i cobrirà tot els serveis i programari d'acord a l'objecte del contracte i els requeriments tècnics.

El servei normal de suport i manteniment haurà de cobrir dies i horari laboral de 9:00 a 14:00 i de 16:00 a 18:00 de dilluns a dijous i de 9:00 a 14:00 els divendres a excepció del 1 de juny al 30 de setembre que l'horari serà de 9:00 a 14:00. El canal d'atenció serà preferentment per mitjans electrònics amb una eina de ticketing d'acord a la metodologia ITIL. També caldrà disposar d'un canal telemàtic fora d'horari normal en cas d'incidència greu o molt greu durant les 24 hores i els 365 dies de l'any.

El servei atindrà tant les incidències tècniques com consultes funcionals dels interlocutors municipals autoritzats sense cost addicional. El servei de suport serà realitzat de forma remota si s'escau per part del contractista d'acord a les indicacions dels tècnics municipals mitjançant connexió segura d'acord a les polítiques de seguretat municipal.

Aquest suport tècnic incorporarà les 'millores' i actualitzacions segons criteris d'universalitat de la solució sense preu addicional. També inclourà la correcció de qualsevol mal funcionament o disfunció del servei o programari i qualsevol parxe, nova revisió, subversió o versió. Inclourà tots els canvis normatius de rang europeu, estatal o autonòmic que es produeixin que afectin al servei contractat i en especial en matèria de signatura electrònica o biomètrica, administració electrònica, interoperabilitat i ciberseguretat. Aquests canvis seran entregats per part del contractista a la corporació municipal sense que aquest últim hagi de destinar recursos d'assessorament, amb temps suficient per validar la seva funcionalitat i sempre abans de l'entrada en vigor dels canvis normatius.

6. ACORDS DE NIVELL DE SERVEI



L'adjudicatari haurà de complir, com a mínim, els acords de nivell de servei mensuals proposats (SLA) i a les penalitzacions previstes en cas d'incompliment següents:

ACORDS DE NIVELL DE SERVEI (SLA)		
CONCEPTE	SLA SOL·LICITAT	PENALITZACIONS SOL·LICITADES
Temps màxim de resolució d'una incidència lleu	< 10 dies laborals	Infracció lleu entre 10 i 15 dies laborals i infracció greu quan es superior a 15 laborals
Temps màxim de resolució d'una incidència greu	< 32 hores naturals	Infracció lleu entre 32 hores i 72 hores naturals i infracció greu quan és superior a 72 hores naturals
Temps màxim de resolució d'una incidència molt greu	< 8 hores naturals	Infracció greu entre 8 i 16 hores naturals i molt greu quan és superior a 16 hores naturals
Disponibilitat trimestral del servei al núvol	>=99,8%	Infracció greu >= 99,5% i <99,8% i molt greu si <99,5%

Criteris d'aplicació dels nivells de servei (SLA)

- Un dia laboral s'entén passat 8 hores en horari laboral del suport i manteniment i un dia natural s'entén passat 24 hores naturals durant els 365 dies l'any.
- Tots aquests paràmetres s'entenen que hauran de ser assumits per l'adjudicatari a excepció dels casos no imputables a aquest.

Tipus incidència

- S'entendrà per **incidència lleu** aquelles que entorpeixin el treball de l'usuari sense provocar cap parada.
- S'entendrà per **incidència greu** aquella que sigui lleu i a més degradi el sistema i afecti a l'usuari final, en quant no permeti desenvolupar de forma normal la seva



tasca, provocant parades intermitents del sistema. Caigudes intermitents i repetides, caigudes de rendiment que provoquin la parada del desenvolupament de les tasques de l'usuari. Elements que provoquin el reinici reiterat del sistema, etc.

- S'entendrà per **incidència molt greu**, aquelles que son greus i a més afecten molt significativament a l'usuari final de la corporació no podent desenvolupar les seves tasques. Per tant, parada i mal funcionament total del sistema.

En el cas que la corporació municipal contracti un servei d'auditories de ciberseguretat o d'adequació a l'ENS i el sistema es detecti un incompliment, subsanació o problema de seguretat sempre i quan sigui imputable al contractista, l'empresa ho haurà de resoldre segons el seu impacte d'acord als següents SLAs indicats anteriorment. El nivell de vulnerabilitat o d'incident de seguretat serà determinat per l'Administrador de Seguretat de la corporació municipal de Reus.

7. ELABORACIÓ D'INFORMES DEL SERVEI

El contractista lliurarà trimestralment un seguit d'informes de seguiment del servei i compliment de SLAs diferenciant entitats municipals i també agrupades per una supervisió global, que entregará als tècnics municipals designats prèviament a la reunió trimestral de seguiment del servei que es realitzarà per ambdues parts que es podrà fer telemàtica o presencial segons acordin les parts.

La data límit de presentació dels informes serà el dia 25 del mes posterior al compliment del trimestre i si és festiu, l'endemà laborable. No es podran presentar ni s'acceptaran factures mentre no s'hagin presentat els informes de seguiment del trimestre i s'hagi fet la reunió trimestral de seguiment.

Adicionalment i sota demanda per part dels tècnics municipals, es podran demanar nous informes orientats a realitzar un control, seguiment i millora de la gestió dels serveis.

Els aspectes a incloure com a mínim en els informes són:

- Informe d'incidències, peticions i actuacions correctives i preventives realitzades així com compliment dels SLA's.
- Propostes de millores orientades a reduir incidències o incorporació de noves funcionalitats o planificació de formacions o actualitzacions.



8. MODIFICACIONS DEL CONTRACTE

Durant la durada del contracte, es podran realitzar modificacions a l'alça o la baixa en un màxim del 20% (IVA exclòs) el pressupost per l'augment o decrement de dispositius biomètrics que usen el servei, pels certificats digitals de personal municipal que tenen el certificat al núvol per signar electrònicament o pel nombre de signatures amb doble factor o electròniques realitzades.

9. FACTURACIÓ

La facturació es presentarà trimestralment i electrònicament d'acord a la normativa vigent a partir de la conformitat dels serveis prestats una vegada finalitzat el trimestre per cada entitat municipal a que se li presti el servei de forma distribuïda. Se signarà una acta d'inici de servei, deixant constància del compliment de requisits a partir de la qual comptarà com inici prestació del servei i de facturació.

10. CONFIDENCIALITAT

L'empresa adjudicatària queda expressament obligada a mantenir absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer amb ocasió del compliment del contracte, especialment les de caràcter personal o confidencial.

L'empresa adjudicatària quedarà obligada a la no difusió de cap tipus de codi d'accés o qualsevol altre tipus d'informació que pugui facilitar l'entrada als sistemes de la corporació municipal, així com a no fer un ús incorrecte dels permisos i privilegis que es concedeixin al seu personal per a l'execució d'aquest contracte.

L'empresa adjudicatària es farà responsable dels perjudicis que se li puguin ocasionar a la corporació municipal degut a d'incompliment de qualsevol de les condicions esmentades.

Per tal de garantir la confidencialitat de la informació i documentació facilitada, el licitador haurà de redactar i signar una declaració de confidencialitat.

Aquesta declaració haurà de ser necessària i proporcional a la finalitat o interès que es vol protegir i ha de determinar de forma expressa i justificada els documents i/o les dades facilitades que considerin confidencials. No s'admeten



declaracions genèriques, sense referència a documents o apartats concrets, o no justificades del caràcter confidencial.

En cas de manca d'indicació, s'entendrà que la documentació no té caràcter confidencial.

De conformitat amb l'article 133.1 de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic, l'òrgan de contractació no podrà divulgar la informació facilitada pels licitadors indicada de forma expressa i justificada, per aquests com a confidencial.

11. PROTECCIÓ DE DADES PERSONALS I SEGURETAT TIC

En el cas que la prestació dels serveis, suposi la necessitat d'accés a dades de caràcter personal, el contractista, com a encarregat del tractament, queda obligat a garantir el compliment de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals i el Reglament (UE) 2016/679 General de Protecció de Dades, així com qualsevol altra normativa vigent nacional i europea en matèria de Protecció de Dades de Caràcter Personal.

El contractista respondrà de totes les infraccions en que podria incórrer en el cas que destini les dades personals a una altra finalitat, les comuniqui a un tercer no autoritzat, o en general, les utilitzi de forma irregular, així mateix quan no adopti les mesures corresponents per l'emmagatzematge i custòdia dels mateixos. A tal efecte, s'obliga a indemnitzar a la corporació municipal, per qualsevol dels perjudicis que sofreixi directament o per tota reclamació, acció o procediment, que porti la seva causa per incompliment o compliment defectuós per part de l'adjudicatari del dispostat tant en el contracte com en la normativa reguladora de la protecció de dades de caràcter personal.

El contractista únicament tractarà les dades de caràcter personal als que pugui tenir accés conforme a les instruccions municipals i no els aplicarà o utilitzarà amb una finalitat diferent a l'objecte del contracte.

El tractament de les dades que pugui originar-se al llarg de l'execució del contracte per part del contractista haurà de realitzar-se a la Unió Europea.

De conformitat amb l'article 122.2 de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic, l'adjudicatària haurà de presentar abans de la formalització del contracte una declaració indicant la ubicació dels servidors i des d'on es prestaran els serveis associats als mateixos. El contractista haurà de



comunicar qualsevol canvi que es produeixi al llarg de la vida del contracte sobre dita declaració. En cas que l'adjudicatària tingui previst subcontractar els servidors o els serveis associats als mateixos, haurà d'indicar a la seva oferta el nom o perfil empresarial dels subcontractistes.

L'empresa caldrà que adopti les mesures tècniques i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat, atès que els elements tecnològics objecte del contracte hi seran exposats així com l'acció humana.

Les anteriors obligacions i altres obligacions addicionals en matèria de protecció de dades personals hauran de regular-se mitjançant la signatura d'un contracte de tractament de dades entre l'entitat municipal corresponent i el contractista.

Caldrà que el servei al núvol, compleixi el RD 311/2022 per al que es regula l'Esquema Nacional de Seguretat en la categoria mitja i se sotmeti a les auditories municipals que siguin oportunes d'acord al compliment de la normativa i en cas de deficiències, a corregir-les sense cost addicional d'acord al nivell de seguretat de les dades que gestioni.

Haurà de disposar d'un pla contingència davant desastres (DR), servei d'alta disponibilitat amb redundància, pla de continuïtat i seguretat física i lògica i presentar-ho en la documentació tècnica del present plec i quines polítiques de seguretat i de còpies de seguretat aplica que siguin conformes a la normativa i a les polítiques de seguretat municipal.

12. MODEL DE PROPOSTA TÈCNICA

Independentment de la documentació de tipus administratiu sol·licitada, els licitadors presentaran la següent documentació obligatòria de caràcter tècnic seguint estrictament el següent guió per acreditar el compliment de requisits:

- 1.- Característiques comunes de la plataforma
- 2.- Característiques del servei de signatura biomètrica
- 3.- Característiques del servei de signatura amb doble factor
- 4.- Característiques del servei de signatura electrònica al núvol
- 5.- API i aplicacions de mercat integrades.
- 6.- Formacions i posada en marxa del servei



AJUNTAMENT DE REUS

PARTICIPACIÓ, BON GOVERN I SERVEIS GENERALS
Servei de Tecnologies de la Informació
i Telecomunicacions
Av. de la Cambra de Comerç 42 -1r pis
Edifici CEPID 43204 REUS
Tel. 977 010 055 Fax 977 010 238
info.stit@reus.cat
www.reus.cat

- 7.- Característiques del servei tècnic de suport, manteniment i actualització
- 8.- Mesures de seguretat TIC, ENS i compliment de la normativa de protecció de dades de caràcter personal
- 9.- Altres aspectes addicionals que es considerin oportuns

Oscar Hellín Escribano
Coordinador del Servei de Tecnologies
de la Informació i Telecomunicacions