



**PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA
CONTRACTACIÓ D'UN SERVEI DE CUSTÒDIA I SIGNATURA
CENTRALITZADA BASADA EN CERTIFICATS DIGITALS EN MODALITAT
PROGRAMARI COM A SERVEI (Software As A Services SAAS). EXP.: SEC
2025 18.**

1. OBJECTE DEL CONTRACTE

En els processos de signatura electrònica implantats en l'Ajuntament de Sant Just Desvern es necessita un sistema per realitzar signatura i autenticació remota.

Per donar resposta a aquest requisit es necessària la contractació d'un servei per emetre certificats, per a la gestió centralitzada i segura dels certificats i dels elements necessaris per a l'ús dels mateixos i que permeti la seva integració amb els sistemes informàtics de l'Ajuntament

L'objecte d'aquest plec és la contractació d'un servei d'emissió directa dels certificats en la plataforma i de custòdia dels certificats emesos, centralitzat i basat en un model SaaS dimensionat segons els nombre d'usuaris i certificats a gestionar. Es tracta d'un sistema de signatura centralitzada basada en un model SaaS. En l'abast del contracte s'inclourà el desplegament necessari del servei en la part del sistema centralitzat en els clients de l'Ajuntament i tots els elements de programari necessaris per a la implantació del servei i la formació, així com la generació de tots els certificats necessaris.

2. PRESTACIONS DEL CONTRACTE

2.1. Servei de sol·licitud de certificats

L'empresa licitadora ha de ser una Autoritat de Registre (RA) habilitada i acreditada per un prestador qualificat de serveis de certificació per a la gestió de tot el cicle de vida dels certificats digitals especificats en aquest plec.

L'empresa licitadora haurà de constituir a l'Ajuntament de Sant Just Desvern com a una Oficina de Verificació Presencial (OVP) de l'Autoritat de Registre (AR) i amb aquesta acció es facultarà a l'Ajuntament per a la emissió de certificats digitals qualificats d'empleat públic.

El procés de constitució com a OVP per part de l'Ajuntament ha de ser un procediment ràpid i simple i cal especificar com es farà aquest procés. L'Ajuntament, com a OVP ha de ser capaç de gestionar i controlar tot el cicle de vida dels certificats especificats en aquest plec, de forma directa i autònoma.

El procés de constitució com a OVP ha de complir amb totes les garanties jurídiques necessàries perquè els certificats qualificats sol·licitats d'empleat públic compleixin amb tota la normativa aplicable per l'ús del certificat electrònic de l'Administració Pública i de forma especial el Reglament (UE) n° 910/2014 del Parlamento Europeo i



del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas (eIDAS).

La responsabilitat de l'Ajuntament de Sant Just Desvern com a OVP serà la d'identificar i personar a les titulars dels certificats digitals i recollir les evidències d'aquests procés i sol·licitar l'emissió del certificat corresponent a la RA (de l'empresa adjudicatària) d'acord amb els procediments establerts per aquest fi.

L'empresa adjudicatària facilitarà a l'Ajuntament de Sant Just Desvern el programari necessari per gestionar i controlar totes les sol·licituds de certificats realitzades.

Aquest programari estarà desenvolupat en entorn Web i serà accessible amb un navegador web sense cap més requeriment que el de garantir l'accés amb identificació segura i amb els registres d'accessos i peticions que siguin necessaris pel correcte funcionament, lògic i jurídic, del procés de sol·licituds.

Aquest programari Web no requerirà cap instal·lació addicional pel seu funcionament i es constituirà com el canal de comunicació entre la RA i la OVP i permetrà també la gestió de tot el cicle de vida dels certificats per part de la OVP, així com realitzar totes les tasques necessàries en el procés.

2.2. Servei de generació de certificats centralitzats

El sistema proposat tindrà els mecanismes necessaris per generar certificats electrònics qualificats (de treballador/a públic/a i de segell electrònic), homologats pel Ministerio de Economía y Empresa

(<https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx>) de manera que la clau privada es generi en el mateix dispositiu segur de creació de signatures (HSM) on quedarà custodiada per a ser utilitzada. També s'haurà de garantir que no es pot exportar la clau del dispositiu HSM.

Els certificats es generaran en la mateixa plataforma i s'incorporaran sense cap intervenció externa al repositori que cada persona tindrà en la plataforma. Caldrà fer una proposta de com es realitzarà la distribució del PIN d'accés al certificat i dels codis dels usuaris per garantir que ho rep la persona destinatària del certificat.

Aquest sistema ha de tenir les mesures de seguretat equivalents a les establertes en l'annex II del Reglament (UE) N° 910/2014.

2.3. Sistema de custòdia de certificats centralitzada

La solució ha de presentar seguretat jurídica mitjançant la utilització de certificats digitals, per assegurar la validesa legal de la documentació signada per mitjans electrònics, alhora que ha de tenir una alta usabilitat, minimitzant la complexitat tecnològica dels sistemes de signatura electrònica basada en certificats digitals, eliminant la dependència del sistema d'elements aliens a la persona usuària.



La generació de les claus associades al certificat i de les claus de xifratge per custodiar-les s'ha de fer en un dispositiu de maquinari, tipus HSM, FIPS 140-2 L3 o amb un nivell de seguretat equivalent o superior.

La proveïdora del servei ha de garantir el seu funcionament de manera que sigui accessible i usable, encara que falli algun dels seus elements. Igualment haurà de tenir capacitat llicenciada per gestionar un mínim de 800 certificats d'empleat públic (5 per usuari/ària) complint els requeriments que s'exigeixen a través d'un Acord de Nivell de Servei (SLA) que es descriu més endavant. El servei prestat ha de posar en funcionament l'ús d'unes claus de signatura basades en tecnologia PKI, que siguin custodiades garantint el control exclusiu de les mateixes per part del propietari del certificat de signatura qualificat.

Per accedir a cada certificat, cada usuari podrà instal·lar en el seu equip el programari client que l'empresa licitadora faciliti. L'accés al magatzem de certificats requerirà un inici de sessió amb validació. El programari ha de facilitar que els certificats als que cada persona tingui accés siguin mostrats com si estiguessin instal·lats en el magatzem de certificats de Windows en el cas d'us en aquest sistema operatiu.

La solució presentada aportada per l'empresa adjudicatària ha de permetre la integració amb els sistemes d'informació amb els que actualment es realitza la generació dels documents a signar. Aquests sistemes estan desenvolupats sobre entorns Windows.

Igualment, ha de permetre la integració amb els serveis de signatura automatitzada que es realitzen des de servidors. Aquesta integració caldrà efectuar-la també en els sistemes clients propietari de l'Ajuntament i l'empresa adjudicatària donarà el suport de desenvolupament necessari per realitzar aquesta integració com s'especifica més endavant en aquest plec.

L'empresa adjudicatària haurà de posar a disposició de l'ajuntament els programaris necessaris que s'hagin d'instal·lar en els ordinadors, servidors, i/o tauletes dels usuaris i dels servidors del servei de custòdia de certificats i la documentació necessària per realitzar les integracions.

Característiques de la plataforma de custòdia de certificats:

- Emmagatzematge centralitzat en el núvol en un entorn d'alta seguretat que compleixi amb tots els requeriments normatius vigents (eIDAS-UE).
- Sistema completament integrat amb la RA del licitador, configurat amb un procés automatitzat i segur d'emissió directa a la plataforma de custòdia càrrega i disponibilitat del certificat.
- Gestió centralitzada del cicle de vida dels certificats (renovacions, revocacions, bloqueig, suspensió, caducitats, etc.).
- Definició i control de les polítiques d'ús dels certificats



- Definició y control dels permisos d'accés, incloent sistemes d'autenticació robusta i de doble factor.
- Disponibilitat del certificat des de múltiples entorns i dispositius.

La plataforma proposada haurà de disposar de dues parts elementals:

- Una consola d'administració centralitzada. L'accés a aquesta consola serà via web i no es requerirà cap programari addicional per connectar-se. Des d'aquesta consola cada persona usuària titular d'un certificat podrà gestionar el seu certificat centralitzat.

Els/Les usuaris/àries administradors/res tindran accés a aquesta plataforma per a la gestió dels/de les usuaris/àries i dels seus certificats, així com per consultar el registre complet de la seva activitat i per a la configuració de les polítiques d'ús dels certificats personals. L'accés a la consola d'administració centralitzada amb el rol d'administrador/a, només utilitzable per a la (es) persona (es) designades pels/per les responsables de la contractació, permetrà la gestió de forma segura de les tasques d'administració, així com l'auditoria i traçabilitat, de les accions realitzades amb tots els certificats associats a aquest contracte.

- Una aplicació d'escriptori basada en CSP (proveïdor de serveis de criptografia), que romandrà en execució una vegada iniciada la sessió. Aquesta aplicació habilitarà l'ús del certificat centralitzat com si estigués emmagatzemat en el repositori de certificats de l'ordinador (per ordinadors amb sistema operatiu Windows)

Amb aquest programari l'usuari/ària podrà tenir accés als certificats centralitzats als quals té permís d'accés i seleccionar el que vol utilitzar. El programari li ha de demanar un PIN (o altres mitjans d'identificació que el propi usuari pugui haver establert) per autoritzar l'ús del certificat.

2.4. Serveis de signatura electrònica

- Signatura centralitzada.

La plataforma ha d'oferir serveis de generació de signatura avançada en la mateixa plataforma on estiguin custodiats els certificats. També ha de permetre completar les signatures realitzades amb segell de temps. S'han de poder generar signatures CADES i completar-les amb segell de temps per generar signatures CADES – LTA, així com els mateixos processos per als formats XAdES i CADES amb les extensions XAdES-LTA i PAdES-LTA.

Els serveis de segell de temps es consumiran en format SaaS i no caldrà la instal·lació de cap programari ni maquinari addicional. El segell de temps seran segells de temps qualificats segons el reglament eIDAS.

També caldrà incloure els servei de custòdia dels segells de temps per un període mínim de 2 anys.



- Signatura amb segell d'òrgan.

El sistema ha de permetre la utilització de certificats per a la realització de signatura automatitzada des de servidors, com per exemple ús de certificats de segell d'òrgan. Els certificats de segell d'òrgan hauran d'estar custodiats també en la plataforma i han de permetre l'ús tant en la signatura automàtica en la pròpia plataforma com en els processos automatitzats de signatura amb segell d'òrgan des dels servidors de l'ajuntament.

- Signatura PIN + sobre digital

La plataforma ha d'oferir serveis de signatura PIN..

Ha de permetre realitzar enviaments manuals, amb càrrega massiva d'enviaments amb arxius preexistents o mitjançant plantilles, a més de permetre una connexió via API per integrar directament amb el programari propi de l'ajuntament.

A nivell de seguretat ha de tenir doble factor d'autenticació, i connector per a connexió single sign-on.

També ha de disposar d'una configuració de grups d'usuaris i rols per poder assignar diferents permisos i funcionalitats.

Funcionalment, la plataforma haurà de contemplar l'enviament i seguiment de serveis d'identitat, formalització de documents amb diferents mètodes de signatura, i serveis de comunicació, com ara des d'enviar un SMS o email certificat, fins a comunicacions amb garantia de recepció, burofaxos electrònics i postals.

Els processos dels serveis electrònics que s'operin a la plataforma amb de disposar del mateix full d'estil que l'ajuntament (logotip, colors, tipus de text) per a que els destinataris ens puguin identificar clarament.

La plataforma ha de contemplar la possibilitat de realitzar els avisos als destinataris per iniciar el procés mitjançant SMS, email i Whatsapp, i permetre definir diferents textos en el cos dels emails d'avís de manera autònoma (sense desenvolupaments tècnics) en funció del tipus d'enviament que es desitja realitzar.

Per als serveis de formalització de documents, la plataforma ha de comptar amb la definició de formularis i la identificació del signant amb la validació del document d'identitat prèvia a la signatura del contracte, que només s'activarà si la validació ha superat els filtres indicats a la pròpia plataforma.

Per tal de controlar els enviaments, la plataforma ha de disposar d'un panel de seguiment dels enviaments on poder cercar per dates, situació, servei, unitat organitzativa, DNI del destinatari, nom del destinatari, referència identificativa de l'ajuntament i poder accedir a la documentació associada a l'enviament o realitzar una descarrega automàtica de la documentació dels registres seleccionats a la cerca, o via API.



2.5. Tipus i usos dels certificats

Les característiques comunes a tots els perfils de certificats són:

- Certificat segons estàndard X.509 versió 3
- Tipus de clau i algoritme de signatura RSA 2048 bits – SHA -256

Els certificats de les Autoritats de Certificació (AC) que serveixin per generar tots els certificats que l'empresa adjudicatària proveeixi a l'ajuntament hauran d'estar admesos (precarregats) en els navegadors estàndards, com a mínim: Navegadors de Microsoft, Apple i Android i els Navegadors Chrome i Mozilla

L'empresa licitadora prestarà servei d'emissió i generació dels següents tipus de certificats:

- Certificat d'empleat públic
 - Certificats qualificats emesos d'acord amb els requeriments establerts en l'article 43 de la Llei 40/2015, d'1 d'octubre, de Règim jurídic del sector públic.
 - Emès pel període de la vigència del contracte.
- Certificat de representant legal
 - Emès pel període de la vigència del contracte
- Certificat de segell d'òrgan
 - Certificat qualificat emes d'acord amb les especificacions l'article 40 de la Llei 40/2015, d'1 d'octubre, de Règim jurídic del sector públic.
 - Emès pel període de vigència del contracte o superior
- Certificats de servidor web (SSL) i de seu electrònica.

Han d'estar emesos per l'empresa adjudicatària, com a prestador qualificat de serveis de Confiança.

S'han de poder emetre certificats SSL dels següents tipus:

- SSL Extended Validation (EV), amb els requeriments del CA/Browser Forum establerts en el document "Guidelines for the issuance and management of Extended Validation certificates".



- SSL Organization Validation (OV), amb els requeriments del CA/Browser Forum establerts en el document “Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates”.
- Els Certificat de seu electrònica ha de ser emès d’acord amb l’article 38 de la Llei 40/2015, d’1 d’octubre, de Règim jurídic del sector públic.
- S’haurà de poder aplicar la protecció de diversos noms de host amb un sol certificat SSL de qualsevol dels tres tipus (EV, OV o Seu electrònica), amb certificat multidomini.
- Addicionalment, en els certificats SSL OV es podrà aplicar el mecanisme Wildcard per a certificats d’un domini i els seus subdominis, facilitant l’ús del caràcter asterisc per a comodí en la URL
- Emès per un període vàlid d’un any

Els suports dels certificats proveïts per l’empresa adjudicatària seran els següents;

- En el cas de certificats d’empleat públic i de representant legal:
 - Suport de programari amb custòdia a la plataforma de l’empresa adjudicatària.
 - Suport en targeta o token criptogràfic (en el cas de requerir signatura qualificada en algun certificat)
- En el cas de certificats de segell d’òrgan:
 - Suport de programari amb custòdia a la plataforma de l’empresa adjudicatària o custòdia en els servidors de l’ajuntament.
- En el cas de certificats de servidor web i de seu electrònica:
 - Suport en programari a instal·lar en el lloc web corresponent.

L’ús dels certificats d’empleat públic i de representat legal serà d’autenticació i signatura electrònica avançada. Aquests usos han de quedar garantits en les plataformes de treball usuals de les administracions públiques catalanes, principalment la plataforma EACAT i el portal de tramitació de la Diputació de Barcelona.

La generació de signatura electrònica d’aquests certificats ha de quedar garantida en les aplicacions desenvolupades per l’ajuntament (d’acord amb les funcionalitats d’integració esmentades més endavant) i en la signatura de les eines ofimàtiques habituals, especialment Microsoft Word i Adobe PDF.

La generació de signatura de segells d’òrgan ha de quedar garantida en processos automatitzats en la plataforma de signatura de l’empresa adjudicatària i en servidors



locals de l'ajuntament de Sant Just Desvern. Els processos automatitzats estaran integrats amb les aplicacions desenvolupades a l'ajuntament (d'acord amb les funcionalitats d'integració esmentades més endavant). Els serveis d'integració han de permetre enviar automàticament els paràmetres i dades necessàries per a la generació de la signatura CAdES – LTA detached a la plataforma adjudicatària i recollir el fitxer de la signatura de forma segura una vegada completada la mateixa.

Les signatures electròniques generades amb els serveis objecte del contracte (certificats i signatures) s'hauran de validar en els serveis de validació que ofereixen els organismes oficials. El format de signatura que caldrà validar serà CAdES – LTA detached. Aquestes signatures generades en la plataforma s'hauran de poder validar (amb el document original) per terceres persones en les plataformes que s'especifiquen en aquest punt i la validació es realitzarà amb els serveis web que ofereixen aquestes plataformes o amb la càrrega manual dels documents i signatures en les esmentades plataformes.

Les plataformes on caldrà realitzar aquestes validacions són les següents (publicades el dia de la publicació d'aquests plecs)

- <https://signasuite.aoc.cat/signasuite/inici>
- <https://valide.redsara.es/valide/>

2.6. Serveis d'integració

L'ús dels certificats emmagatzemats de forma centralitzada no requerirà de cap maquinari addicional en els equips, i l'ús del certificat haurà de ser transparent per a l'usuari i podrà ser des de diferents equips.

Per a això l'empresa adjudicatària facilitarà el programari necessari per identificar de forma segura la persona usuària en qualsevol equip. Aquesta identificació i autenticació estarà basada com a mínim amb usuari i paraula de pas. Un cop identificat, l'usuari identificat tindrà a la seva disposició en l'equip en el qual ha s'ha identificat, els certificats digitals que estan carregats a la plataforma, i ells hi té permís sent necessària només la sol·licitud d'un PIN per a l'ús del certificat.

El programari necessari, així com la llicència d'ús durant la prestació del servei per garantir aquesta integració haurà de ser transparent per a l'usuari del certificat, haurà de poder ser instal·lat de forma automàtica i haurà d'estar suportat per la plataforma de clients Windows, deixant disponibles a cada usuari només els certificats emmagatzemats sobre els quals tingui autorització.

La integració en els entorns Windows ha de facilitar la presentació dels certificats disponibles de cada usuari com si estiguessin en el repositori de windows i d'aquesta forma han de quedar disponibles perquè aplicacions de tercers els puguin consumir. L'empresa adjudicatària ha de garantir que la utilització de certificats per aquest mitjà per a la generació de la signatura electrònica es podrà realitzar en la plataforma de l'empresa adjudicatària i amb l'aplicació Signador desenvolupada pel Consorci Administració Oberta de Catalunya (CAOC).



La integració amb sistemes de signatura automatitzades ha de permetre accedir a un certificat de segell electrònic de forma automàtica sense la intervenció de la persona, enviant les dades necessàries per accedir al certificat (usuari/contrasenya, identificador del certificat)

Per a la integració dels processos de signatura electrònica amb els certificats objecte d'aquest contracte, el sistema ha de disposar dels elements necessaris, com ara Webservices i/o APIs, que permetin la integració de les aplicacions (per a certificats d'empleat públic i de segell d'òrgan). Aquests serveis d'integració han de permetre la signatura múltiple de documents amb una sola crida als serveis d'integració (Webservice o APIS) mínim 10 documents per crida.

Les empreses licitadores han de presentar un pla d'integració on cal especificar com a mínim:

- Estimació de dedicació que les empreses licitadores requeriran del personal tècnic de l'ajuntament per realitzar la integració.
- Calendari detallat de les actuacions previstes en la integració així com el termini de les mateixes. Ha de quedar especificat el termini total previst de la integració.
- Especificacions tècniques de l'arquitectura de programari de la integració
- Detall del format del programari d'integració especificant les crides a realitzar via API's o Web Services així com la forma de la resposta d'aquestes funcions

Les empreses licitadores podran sol·licitar al servei d'informàtica de l'ajuntament la informació necessària per realitzar el pla d'integració.

La integració caldrà realitzar-la en el programari de gestió d'expedients propi de l'ajuntament i en els serveis de validació de signatura de la seu electrònica de l'ajuntament. El programari utilitzat en aquests desenvolupaments per part de l'ajuntament és Microsoft .NET i la integració caldrà realitzar-la amb aquesta tecnologia.

L'oferta ha d'incloure tots els costos econòmics i la valoració de recursos associats als treballs d'integració amb les aplicacions que l'ajuntament té integrades actualment. Aquests costos d'integració seran a càrrec de l'empresa adjudicatària.

2.7. Serveis d'implantació i formació

Els treballs de posada en marxa de la solució adjudicada han de contemplar la substitució de la solució de signatura electrònica desplegada actualment. Es contemplen dues tasques principals:

- La desinstal·lació del programari client desplegat actualment en 160 equips.
- La instal·lació del programari de la solució adjudicada en 160 equips.



El servei d'Informàtica de l'Ajuntament de Sant Just Desvern facilitarà a les empreses licitadores que ho sol·licitin la informació necessària perquè les empreses licitadores puguin valorar aquestes tasques.

L'oferta ha d'incloure tots els costos econòmics i la valoració de recursos associats als treballs de substitució de la solució desplegada actualment i del desplegament de la solució adjudicada, a càrrec de l'empresa adjudicatària.

El licitador haurà de presentar un pla de desplegament del servei (pla d'implantació), incloent estimació de temps de totes les tasques a realitzar, que inclogui no només la posada en marxa de la solució aportada, sinó també la formació dels diferents actors dins de la solució. Caldrà especificar en el pla d'implantació com es realitzarà per què puguin conviure el sistema desplegat actualment amb el sistema adjudicat, de forma que no quedi interromput el servei de signatura electrònica desplegat actualment. Aquests treballs hauran d'estar finalitzats en un màxim de tres mesos des de la formalització del contracte.

Les empreses licitadores han de presentar un pla d'implantació on cal especificar com a mínim:

- Estimació de dedicació que les empreses licitadores requeriran del personal tècnic de l'ajuntament per realitzar la implantació.
- Calendari detallat de les actuacions previstes en la implantació i terminis de les mateixes. Ha de quedar especificat el termini total previst de la implantació.
- Especificacions detallades de com es realitzarà la desinstal·lació dels programari client actual i com s'instal·larà el nou.
- Especificacions detallades de com es realitzarà el desplegament del servei per garantir que el servei actual no quedarà interromput.
- Calendari detallat de la formació i detall del contingut de la formació

2.8. Serveis de suport

Suport a tècnics de sistema

L'adjudicatari haurà de donar suport específic al personal tècnic de l'Ajuntament que estigui al càrrec de la gestió del sistema de custòdia de certificats i autenticació per solucionar els dubtes i incidències que puguin produir-se en el sistema.

Serà responsabilitat de l'adjudicatari les comunicacions que hagin de realitzar amb tercers sobre incidències de cada un dels elements, tant maquinari com programari, del sistema de custòdia i autenticació.

Durant tota la vigència del contracte l'empresa licitadora donarà servei de suport a les integracions realitzades pel personal tècnic de l'Ajuntament.



Aquest servei estarà subjecte a les condicions que s'estableixin en l'Acord de nivell de servei (SLA) que es detallen més endavant.

Aquest suport serà com a mínim en la modalitat 5x8 i serà vigent durant tota la durada del contracte i els canals de comunicació amb el servei de suport seran correu electrònic i plataforma web com a mínim.

3. ACORD DE NIVELL DE SERVEI

Tant la plataforma de custòdia de certificats com l'emissió dels certificats estaran subjectes al compliment de la següent taula de Nivell de servei, sempre que les incidències no siguin atribuïbles a operacions o elements externs a la solució (exemple, talls de subministrament elèctric, talls de xarxa de dades aliena a la solució, operacions de manteniment programades, etc.).

Bloc de servei	indicador	criticitat	Param. mesura	valor màxim
Gestió d'incidències	Temps mitjà d'atenció davant incidència	Alta	minuts	90
		Mitjana	hores	2
		baixa	hores	8
	Temps mitjà de resolució davant incidència	Alta	hores	16
		Mitjana	hores	24
		baixa	hores	48
	Informe mensual		Data de lliurament	5 primers dies laborals del mes
Bloc de servei	indicador	criticitat	Param. mesura	valor màxim
Consultes de suport	Temps mitjà de resposta		hores	6

Per a la classificació de les incidències s'utilitzaran els següents criteris:

- Criticitat Alta:
 - Qualsevol pèrdua crítica o altament significativa de la disponibilitat del servei que creï una situació d'impacte crític:
 - Servei no disponible o que no pot ser utilitzar pels usuaris
 - Pèrdua total del servei
 - No disponibilitat de components crítics (infraestructura o programari) que puguin derivar en la pèrdua total del servei.
- Criticitat mitjana:
 - Qualsevol incidència que impacta en una pèrdua parcial del servei però permet tenir disponible els serveis mínims necessaris:
 - Fallada en algun component no crític del sistema (infraestructura o programari)



- Incidències puntuals que disposin d'un marge temporal per a la seva resolució o que el seu impacte sigui mínim.
 - El funcionament del servei es vegi degradat mínimament.
 - Quan un incident pugui ser potencialment crític si no es resol.
- Criticitat baixa:
 - Qualsevol incidència que no impacta en un a pèrdua total o parcial del servei que pots ser reparada sens urgència

Els incompliments del SLA es tractaran com a un incompliment greu del contracte especificats en el plec de condicions administratives.

4. TERMINI DE LA GARANTIA

El període de garantia serà exactament el de durada del contracte i començarà a comptar a partir de la data d'inici de prestació de serveis.

5. LLIURAMENT I SUBMNISTRAMENT

Els treballs d'integració i d'implantació s'executaran a partir del dia següent al de la data de signatura del contracte d'acord amb els Plans d'integració, implantació i formació presentats per l'empresa adjudicatària.

6. GESTIÓ DE LA CAPTIVITAT

En el moment de la finalització del contracte l'empresa adjudicatària facilitarà a l'Ajuntament tots els logs de sistemes i d'auditories disponibles.

L'adjudicatària també ha de garantir, amb una declaració responsable, l'eliminació de tots els certificats i claus del sistema. Aquesta declaració responsable inclourà el llistat de tots els certificats eliminats identificant el certificat i la persona que el tenia assignat.

Finalment, l'adjudicatària facilitarà a l'Ajuntament altres elements que per a l'ús dels serveis motiu d'aquest contracte tinguin en els seus sistemes d'informació.

Andrés Torralbo Sepúlveda
TÈCNIC DE SUPORT DE SISTEMES
I PROGRAMADOR INFORMÀTIC

Sant Just Desvern, en la data de la signatura electrònica.
Ref.: SEC 2025 18 2