



**Ajuntament
de Barcelona**

Institut Municipal d'Informàtica
Direcció de Serveis de Desenvolupament

**PLEC DE PRESCRIPCIONS TÈCNIQUES PER AL
SUBMINISTRAMENT D'UNA PLATAFORMA LOWCODE
DE DESENVOLUPAMENT D'APLICACIONS PER
L'AJUNTAMENT DE BARCELONA, AMB MESURES DE
CONTRACTACIÓ PÚBLICA SOSTENIBLE**



ÍNDEX

1. INTRODUCCIÓ.....	4
1.1. ANTECEDENTS _____	4
1.2. SITUACIÓ ACTUAL _____	5
2. OBJECTE	6
3. ABAST DEL CONTRACTE	6
3.1. PRESTACIONS INCLOSES AL SUBMINISTRAMENT _____	7
3.2. INFORMACIÓ DE LA SUBSCRIPCIÓ A LA PLATAFORMA _____	7
3.3. SERVEIS D'IMPLANTACIÓ I GOVERN DE LA PLATAFORMA _____	8
3.4. EQUIP DE TREBALL _____	11
4. REQUERIMENTS DE LA SOLUCIÓ LOW CODE	11
4.1. REQUISITS MÍNIMS _____	11
4.2. REQUISITS AVALUABLES _____	13
5. ORGANITZACIÓ I MODEL DE RELACIÓ	13
6. CONDICIONS D'EXECUCIÓ	13
6.1. LLOC DE PRESTACIÓ DEL CONTRACTE _____	13
6.2. GARANTIA _____	13
7. FACTURACIÓ.....	14
7.1. PER AL SUBMINISTRAMENT DE LA PLATAFORMA _____	14
7.2. PER LA IMPLANTACIÓ I GOVERN DE LA PLATAFORMA. _____	14
7.2.1. Activació, Planificació i Fundació.....	14
7.2.2. Implementació i Operació Inicial	15
7.2.3. Maduració i Optimització.....	15
8. PROPOSTA TÈCNICA I ECONÒMICA	16
8.1. CONTINGUT DEL SOBRE ELECTRÒNIC B _____	16
8.2. CONTINGUT SOBRE ELECTRÒNIC C _____	18
9. CLAUSULES GENERALS DE SEGURETAT	18
9.1. SEGURETAT DELS SISTEMES D'INFORMACIÓ, PROTECCIÓ DE DADES I COMPLIMENT NORMATIU _____	18
9.2. CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT _____	19
9.3. CLÀUSULA DE PROPIETAT INTEL·LECTUAL _____	19
9.4. CLÀUSULA PER ACCESSOS POTENCIALS _____	20
9.5. CONFIDENCIALITAT _____	20
10. CLÀUSULES IMPLANTACIÓ D'UN PRODUCTE	21



10.1.	GESTIÓ D'IDENTITATS, AUTENTICACIÓ D'USUARIS _____	21
10.2.	AUTORITZACIÓ DELS USUARIS ALS SISTEMES _____	21
10.3.	PROTECCIÓ DE LES APLICACIONS I SERVEIS WEB _____	22
10.4.	ACCEPTACIÓ I POSTA EN SERVEI _____	23
10.5.	DADES DE PROVES _____	23
10.6.	XIFRATGE DE DADES _____	24
10.7.	SIGNATURA ELECTRÒNICA _____	24
10.8.	CERTIFICATS _____	24
10.9.	PLA DE TRACES _____	24
11.	CLÀUSULES ADMINISTRACIÓ.....	25
11.1.	INVENTARI D'ACTIUS _____	25
11.2.	CONFIGURACIÓ DE SEGURETAT _____	25
11.3.	MANTENIMENT _____	26
11.4.	ANTIMALWARE _____	26
11.5.	CÒPIES DE SEGURETAT _____	27
11.6.	CONTROL D'ACCÉS _____	27
11.6.1.	Segregació de funcions i tasques	27
11.7.	EXPLOTACIÓ _____	27
11.7.1.	Gestió de la configuració	27
11.7.2.	Gestió de canvis.....	28
11.7.3.	Protecció de claus criptogràfiques	28
11.8.	PROTECCIÓ DELS SERVEIS _____	28
11.8.1.	Protecció enfront de la denegació de servei.....	28
12.	ANNEXOS	29
12.1.	ANNEX 1. RELACIÓ DE SUBMINISTRAMENTS DEL PRODUCTE LOW CODE ____	29



1. INTRODUCCIÓ

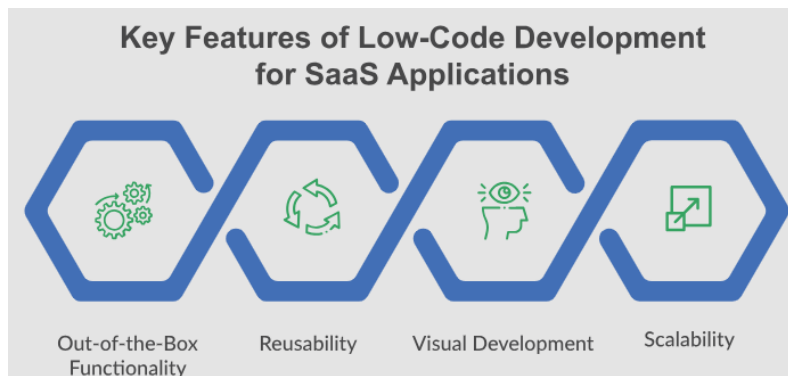
1.1. ANTECEDENTS

El Consell rector de L'Institut Municipal d'Informàtic de l'Ajuntament de Barcelona (IMI en endavant) va aprovar el Pla Estratègic 2024-2030 el dia 19 de febrer de 2024.

Aquesta estratègia tecnològica va ser comunicada a tota l'organització en sessió corporativa el dia 7 de maig de 2024 i fixa els criteris que han de marcar totes les decisions que en aquesta matèria es prenguin a l'IMI, tant per al plantejament de noves solucions, com per al manteniment i evolució de les existents. Es una estratègia Cloud First i es fonamenta en:

- Apostar per solucions administrades sempre que sigui possible (SaaS).
- En els casos on no sigui possible adoptar una solució administrada (SaaS), optar per la implementació de solucions de desenvolupament ràpid (low code)
- En els casos on no sigui possible adoptar una solució de desenvolupament ràpid (low code), optar per la implementació de solucions de desenvolupament a mida Cloud Native.
- Interoperar el conjunt de solucions i governar a la interoperabilitat a través de plataformes d'integració
- Hiper-automatització, que consisteix en l'increment de l'automatització dels processos de negoci introduint intel·ligència artificial (AI), aprenentatge automàtic (ML) i automatització robòtica de processos (RPA).

Atenent al full de ruta de desplegament de l'estratègia és el moment d'entomar el desplegament una infraestructura de Low Code per al desenvolupament ràpid d'aquelles solucions per les quals o bé no és possible trobar una solució de mercat adequada, o bé l'IMI considera que conformen elements de diferenciació i/o innovació i que, per tant, és necessària la inversió en la construcció d'una solució pròpia basada en Low Code.





1.2. SITUACIÓ ACTUAL

La situació actual relativa al Low Code es la següent:

El 8 d'abril de 2024 es lliura un informe, realitzat sota el servei de consultoria dins del Contracte del Manteniment d'Aplicacions d'Arquitectura (expedient número 22000109) amb l'objectiu d'analitzar les plataformes Low Code LCAP Empresariales amb presència al mercat i més ben valorades, la solució millor posicionada en els aspectes valorats va ser OutSystems ([Document annex ARQ-42942-Comparativa Plataformes LowCode.pdf](#)).

Es va realitzar una anàlisi exhaustiva de les principals opcions de plataformes low-code, tenint en compte la seva rellevància, presència de mercat i capacitat per satisfer els requeriments proporcionats per l'IMI.

La selecció de plataformes a analitzar es va realitzar tenint en compte la seva presència com a líders de diferents publicacions de referència, com Gartner o Forrester, durant els darrers anys i on el seu àmbit sigui **Multisectorial i sense limitació per articular cap tipus d'aplicació**.

Es va analitzar el grau de compliment dels següents grups de característiques:

- Grau d'evolució tecnològica
- Experiència d'usuari
- Experiència de desenvolupament
- Pràctiques de DevOps
- Governança
- Migracions i Vendor Locking
- Extensibilitat de plataforma
- Seguretat
- Factors econòmics

El dia 8 de novembre de 2024 es va publicar una consulta preliminar de mercat per tal conèixer quines plataformes donen compliment al grup de característiques relacionades anteriorment i quin seria el preu per licitar la capacitat dels subministraments descrits a l'annex 1 del plec de prescripcions tècniques que acompanya aquest informe. Es van presentar i donar resposta 9 empreses i arrel del resultat de la consulta es va confeccionar un informe amb les dades resultants de la consulta i les conclusions finals ([Document annex Informe final consulta mercat Low Code.pdf](#)).

En la resposta, segons els requisits exposats en la consulta, per la plataforma a seleccionar, 7 empreses van proposar OutSystems Platform, 1 empresa va proposar Mendix i 1 va proposar Appian.



Les 9 propostes van contestar afirmativament als requeriments però algunes no van referenciar les evidències documentals del fabricant. De les respostes tenim la certesa en quant a la viabilitat d'execució de la solució proposada en aquesta licitació i que analitzat el mercat podem satisfer les necessitats tècniques de l'Ajuntament en relació a aquest objecte.

Tant el pressupost com la relació de subministraments continguda a l'annex 1 del present plec de prescripcions tècniques, s'han elaborat tenint en compte el resultat de la consulta preliminar, en base a les respostes que en la resposta van proposar la *plataforma OutSystems* doncs les altres dos propostes van donar preus per modalitats i capacitats de llicenciamnt diferents a les plantejades a la consulta (relació de subministraments a l'annex 1).

2. OBJECTE

L'objecte del contracte és el subministrament d'una plataforma LowCode de desenvolupament d'aplicacions per a l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible.

L'abast de l'objecte del contracte es troba especificat de manera exhaustiva a la clàusula 3 i concordants del present plec de prescripcions tècniques.

El conjunt de subministraments inclosos a l'objecte i abast del present contracte s'enumeren a l'annex 1 del present plec de prescripcions tècniques.

3. ABAST DEL CONTRACTE

L'objecte de la present contractació inclou l'aprovisionament d'una plataforma Low Code, d'àmbit Multisectorial i sense limitació per articular cap tipus d'aplicació, en mode de llicenciamnt Software as a Service (SaaS), per l'Ajuntament de Barcelona, així com serveis especialitzats en el govern, l'ús i construcció de serveis sobre la plataforma per a complementar amb coneixement expert els projectes que es facin sobre la mateixa en cas que la complexitat ho requereixi. Aquest aprovisionament comprèn el dret d'ús, durant la vigència del contracte, per part de l'Ajuntament per àmbit intern sense facultat de cessió a tercers dels subministraments objecte del contracte.

La plataforma s'oferirà en mode SaaS i haurà de ser una plataforma LowCode de desenvolupament d'aplicacions empresarials, d'àmbit generalista i full stack d'última generació.

La plataforma ha de complir amb tots i cadascun dels requeriments descrits a la clàusula 4 del present plec i oferir-se en la modalitat i amb les capacitats detallades a l'annex 1 del present plec de prescripcions tècniques, per tal d'adaptar-se a les necessitats de les aplicacions de l'Ajuntament de Barcelona i s'ha d'oferir en mode SaaS en un dels tres principals Hiperescalars



del mercat i ha de complir amb tots els requeriments estàndards i de seguretat que estableix l'IMI pels seus serveis al núvol públic.

3.1. PRESTACIONS INCLOSES AL SUBMINISTRAMENT

L'adjudicatari haurà d'incloure necessàriament els següents subministraments i serveis associats:

- a) El lliurament dels subministraments que s'indiquen en l'annex 1 del present plec, acreditant la seva vigència.
- b) Suport professional del fabricant en horari 24 x 7.
- c) Implantació i govern de la Plataforma i dels Desenvolupaments a realitzar sobre aquesta descrits a l'apartat 3.3 del present plec.

3.2. INFORMACIÓ DE LA SUBSCRIPCIÓ A LA PLATAFORMA

L'adjudicatari haurà de lliurar, en l'inici del contracte i com a màxim una setmana després de que s'hagin activat la vigència del subministrament de la plataforma, un fitxer MS Excel® amb el següent format:

Descripció producte	Part Number o SKU	Unitats adquirides	Quantitat per unitat	Mètrica	Cost de compra unitari anual amb IVA	Data efectiva	Data finalització	Data primera adquisició / subscripció del producte	Número de contracte o contracte associat	Fabricant	Proveïdor

Omplint-la completament amb tantes files com productes siguin lliurats segons l'abast demanat en el punt 3 i concordants del present plec.

La descripció dels camps a omplir és la següent:

Descripció producte: Nom del producte segons el fabricant del mateix.

Part Number o SKU: Identificador alfanumèric del producte donat pel fabricant del mateix.

Unitats adquirides: Unitats del producte adquirides segons es demana al plec.

Quantitat per unitat: Omplir quan la mètrica del producte correspongui a un paquet indicant quin és aquest valor (per exemple: 2 quan la mètrica sigui packs de dos processadors)

Mètrica: Descripció de la mètrica corresponent al producte (per exemple: packs de dos processadors o usuaris nominals en cloud)

Cost de compra unitari anual amb IVA: Cost del producte unitari anual amb IVA inclòs.



Data efectiva: Data d'inici de validesa del producte. És a dir, data en què el producte està disponible per a la seva utilització o data en què s'activa el corresponent dret d'ús o manteniment.

Data finalització: Data de fi de validesa del producte. És a dir, data en què el producte ja no està disponible per a la seva utilització o data en què s'acaba el corresponent dret d'ús o manteniment.

Data primera adquisició / subscripció del producte : Data del primer contracte per part de l'IMI de l'adquisició o subscripció del producte.

Número de contracte o contracte associat: És el codi o nom del contracte associat que l'adjudicatari signa o activa amb el fabricant i que conté els termes i condicions del programari.

Fabricant: Fabricant del producte.

Proveïdor: Adjudicatari del contracte.

Juntament amb aquest document en format MS Excel®, l'adjudicatari lliurarà els termes i condicions del programari que aplica pels productes demanats. Tant el fitxer en format MS Excel® com aquesta documentació no han de ser incloses juntament amb l'oferta, sinó quan el licitador esdevingui adjudicatari del contracte i els productes s'hagin activat i/o lliurat.

És requisit imprescindible que aquesta informació sigui lliurada correctament per poder presentar la facturació del contracte, podent ser motiu de penalitzacions si no es compleix el seu lliurament en el termini establert.

3.3. SERVEIS D'IMPLANTACIÓ I GOVERN DE LA PLATAFORMA

Aquests serveis engloben tots aquells imprescindibles per la Implantació i el govern de la plataforma i dels desenvolupaments que es realitzin sobre aquesta.

Per a la Implantació i el govern de la plataforma i dels desenvolupaments que es realitzin sobre aquesta l'IMI pot requerir la realització de determinades tasques complexes que requereixin de la participació de personal expert en la plataforma amb les certificacions adients.

L'adjudicatari haurà de poder proporcionar els perfils requerits per portar a terme les següents funcions:

0. Activació de la plataforma i connectivitat segura i resiliència

- Activar la plataforma Low Code i garantir que totes les funcionalitats bàsiques estiguin operatives.
- Establir una connectivitat segura i resiliència i amb suficient capacitat entre l'IMI i la plataforma (incloent redundància i monitoratge). Aquesta tasca inclou totes les configuracions i desenvolupaments necessaris fins validar que les crides des de l'origen arriben a l'API Manager Corporatiu.
- Configurar l'entorn inicial amb les eines necessàries per desenvolupar i operar.



1. Creació del programa d'adopció de la tecnologia

- Definició de les línies estratègiques del programa d'adopció i com s'ha de dur a terme, proporcionant els mecanismes de mesura resultats que certifiquin la correcta execució del canvi.

2. Creació i execució del procediment de gestió de la demanda i alineació amb el volum de subministraments subscrits

- Aquesta activitat assegura que cadascuna de les iniciatives és viabilitzada o descartada en funció del ROI, la idoneïtat d'abordar-les amb tecnologies Low Code o els riscos que comporta el seu abordatge.

3. Dur a terme la Gestió del canvi que suposa per l'Organització

- Integrar el Low Code en els processos i equips de l'organització.
- Evangelitzar amb píndoles i documentació tècnica específica.

4. Creació de la Metodologia: Adopció de la metodologia de desenvolupament proposta pel fabricant

Adopció de la metodologia de desenvolupament proposada pel fabricant de la plataforma, adaptada a les necessitats de l'organització.

5. Garantir la disponibilitat, el rendiment i la mantenibilitat de la infraestructura Low Code.

- Gestió de permisos a tot l'ecosistema Low Code.
- Instal·lació de components.
- Gestió de la comunicació amb Suport (incidental, comunicació d'actuacions, informatiu, ...).
- Suport en l'execució de tasques a la plataforma (proves de càrrega/estrès, proves de seguretat, optimització de processos, ...).
- Desenvolupament d'aplicacions internes per a suport al servei de Factory Manager.
- Executar processos/adaptar configuracions en entorn de producció.
- Realitzar actualitzacions de plataforma.
- Monitoritzar la plataforma.
- Resolució d'incidències de plataforma.
- Alta/Baixa d'aplicacions.
- Control i manteniment d'integracions.
- Gestió de CI/CD (suport en promocions entre entorns, passis a Producció).
- Gestió d'usuaris i credencials.



6. Garantir l'alineació amb les polítiques i el full de ruta definit nivell d'arquitectura, seguretat i qualitat.

- Revisió i validació dels diagrames d'arquitectura dels desenvolupaments, juntament amb els arquitectes de l'Organització.
- Suport a equips de desenvolupament amb la concepció de l'arquitectura dels seus desenvolupaments.
- Correcció de problemes de seguretat a la plataforma d'OS.
- Documentació d'activitats i processos del servei.

7. Maximitzar el reaprofitament de components en tots els desenvolupaments.

- Anàlisi i validació de les propostes de desenvolupament.
- Adequació de components per reutilitzar-los.
- Suport a equips de desenvolupament (tècnic, logs, monitorització, solució de problemes,...).
- Actualització de components de plataforma, transversals i de la forge.
- Manteniment de components corporatius.

8. Millora continua del desenvolupament

- Definició i operació DevOps
- Suport als equips de desenvolupament
- Definir i assegurar la qualitat dels desenvolupaments

9. Reutilització

- Govern i creació d'extensions de components transversals, tant UX com d'integració, BackEnd, etc., per a la seva reutilització.

10. Formació a equip IMI pel desenvolupament de totes aquestes funcions

- En acabar el contracte l'equip de l'IMI ha de tenir la formació i coneixements suficients per exercir aquestes tasques de forma autònoma.

Per donar resposta a aquest servei l'adjudicatari proporcionarà personal tècnic certificat per la plataforma Low Code. L'adjudicatari haurà de proporcionar els següents perfils tècnics que hauran de complir amb la solvència tècnica que es relaciona a continuació:

- Cap de projecte/Tech lead: Perfil per liderar tasques d'arquitectura i operacionals. Capaç de dissenyar el nivell d'arquitectura de les aplicacions, el control de qualitat del codi i mapejar les característiques tècniques de les solucions amb els requisits funcionals i no funcionals.



Es requereix certificació, per part del fabricant que acrediti la capacitat segons la motivació i contingut que s'ha expressat a la clàusula 10.2 de l'informe de necessitat que es troba en l'expedient.

- **Consultor/Developer:** Perfil amb capacitat per realitzar tasques tècniques sobre la plataforma, construir i mantenir aplicacions, realitzar test i desplegar les aplicacions.

Es requereix la certificació, per part del fabricant que acrediti la capacitat segons la motivació i contingut que s'ha expressat a la clàusula 10.2 de l'informe de necessitat que es troba en l'expedient.

- **Consultor especialista/Architect:** Perfil especialista d'alt nivell capaç de dissenyar arquitectures complexes tenint en compte totes les variables (capacitat, sostenibilitat, gestió de l'obsolescència i del deute tècnic, costos, integracions, etc.).

Es requereix la certificació, per part del fabricant que acrediti la capacitat segons la motivació i contingut que s'ha expressat a la clàusula 10.2 de l'informe de necessitat que es troba en l'expedient.

A l'oferta econòmica el licitador haurà de presentar un preu unitari per a cada perfil.

3.4. EQUIP DE TREBALL

Perfil	Solvència Tècnica
Un (1) Cap de projecte/Tech lead	4 anys d'experiència en la plataforma Low Code dirigint equips de treball i construint solucions sobre la plataforma. I amb la certificació següent: <ul style="list-style-type: none"> - Certificat del fabricant que acrediti la capacitat com a Tech Lead de la solució proposada.
Un (1) Consultor/developer	4 anys d'experiència en la plataforma Low Code configurant i construint solucions sobre la plataforma. I amb la certificació següent: <ul style="list-style-type: none"> - Certificat del fabricant que acrediti la capacitat com a desenvolupador de la solució proposada.
Un(1) Consultor especialista/Factory Manager/Architect	4 anys d'experiència en la plataforma Low Code liderant el disseny d'arquitectures sobre la plataforma per a la construcció de solucions escalables, interoperables i amb un cicle de vida del programari eficient. I amb la certificació següent: <ul style="list-style-type: none"> - Certificat del fabricant que acrediti la capacitat com a arquitecte o expert devops de la solució proposada.

4. REQUERIMENTS DE LA SOLUCIÓ LOW CODE

4.1. REQUISITS MÍNIMS

Els requeriments base, d'obligat compliment, de la plataforma Low-Code d'última generació a contractar son:



1. La plataforma ha de ser full-stack, d'àmbit Multisectorial no ha de presentar cap restricció ni limitació per articular cap tipus d'aplicació: Aplicacions Corporatives, Departamentals, Portals, Web o Mòbil amb una experiència d'usuari perfecta i adaptada a les normes i estils corporatius.
2. Ha de poder ser consumida en mode SaaS, desplegada amb serveis auto gestionats d'un dels tres principals HiperScalers.
3. Ha d'oferir la possibilitat de ser desplegada on-premise
4. Ha de permetre, de forma àgil, migrar les aplicacions i les seves dades de la plataforma o proveïdor Low Code cap a altre proveïdor o plataforma, sense pèrdua ni degradació de funcionament . En el cas de rescissió de contracte s'ha de rebre el codi font sense la necessitat de fer servir SDKs complexos, amés de no requerir d'entorns propietaris per la seva execució.
5. El SLA de disponibilitat no pot ser inferior al 99,50%
6. El suport del fabricant de la plataforma ha de ser 24x7
7. RPO màxim de 24 hores i RTO màxim de 12 Hores
8. Ha d'estar certificada en ENS (Certificat de conformitat amb l'Esquema nacional de seguretat, per a sistemes de categoria ALTA) i alineada amb la normativa GDPR.
S'acreditarà per qualsevol dels mitjans admesos segons la normativa aplicable.
9. Ha de ser una plataforma full-stack de desenvolupament d'aplicacions i de gestió de tot el cicle de vida. De manera visual ha de cobrir el desenvolupament, la qualitat, el desplegament, el monitoratge i el govern.
10. Ha de permetre crear aplicacions pixel-perfect. Significa poder crear interfícies d'usuari que s'implementen exactament segons la imatge i els principis de disseny corporatius.
11. L'entorn de Desenvolupament no ha de consumir cap subscripció de llicència.
12. Els usuaris externs, no identificats, no han de consumir llicència.
13. La modalitat de subscripció i les capacitats, tant d'usuaris com d'aplicacions, seran las descrites a l'annex 1

Qualsevol d'aquests requisits no cobert suposarà l'exclusió de l'empresa licitadora en aquest concurs públic.



4.2. REQUISITS AVALUABLES

Els requisits que seran objecte de millora a través de criteris de valoració tant de judici de valor com de forma automàtica, s'agrupen dins les següents àrees de valoració:

1. Arquitectura
2. Facilitat d'ús
3. Capacitats de Desenvolupament i ALM
4. Continuitat del Servei
5. Analítica i Monitorització
6. Funcionalitats avançades
7. Ecosistema i suport
8. Reputació del fabricant

5. ORGANITZACIÓ I MODEL DE RELACIÓ

L'IMI gestiona tots els subministraments i serveis de forma centralitzada per part d'un equip encarregat i especialitzat en aquest tema. Aquest equip serà l'interlocutor per part de l'IMI i tindrà la responsabilitat de validar el correcte lliurament dels productes demanats amb el licitador.

El licitador detallarà la seva proposta d'organització per assegurar de forma òptima els subministraments i serveis indicats a la clàusula 3 i concordants del present plec. Com a mínim, oferirà un contacte tècnic expert en llicenciament de la plataforma Low Code i un contacte administratiu que es responsabilitzi dels aspectes comercials i administratius.

6. CONDICIONS D'EXECUCIÓ

A continuació es detallen les condicions d'execució del present contracte.

6.1. LLOC DE PRESTACIÓ DEL CONTRACTE

La prestació de la totalitat de l'abast del contracte es durà a terme des de les instal·lacions de l'adjudicatari i, per tant, aquest haurà d'aportar els medis logístics suficients per a la citada prestació. De manera excepcional, l'IMI podrà demanar el desplaçament de l'adjudicatari a les oficines de l'IMI per a la prestació d'aquell servei que sigui necessari, essent obligació de l'adjudicatari l'aportació de les eines necessàries per a la prestació.

Es considera que no serà necessària la connectivitat amb l'IMI per a la prestació del servei.

6.2. GARANTIA

Ateses les característiques i objecte del contracte no s'estableix període de garantia un cop rebut aquest.



7. FACTURACIÓ

L'adjudicatari lliurarà a l'inici del contracte el subministrament de la plataforma pel total d'usuaris tota vegada que aquesta estigui plenament operativa pel total d'usuaris contractats, l'adjudicatari facturarà el contracte d'acord segons les següents instruccions:

7.1. PER AL SUBMINISTRAMENT DE LA PLATAFORMA

L'adjudicatari facturarà la part corresponent a la primera anualitat del subministrament de la plataforma un cop el subministrament de la plataforma estigui plenament operativa pel total d'usuaris i capacitats contractades.

A l'inici de les successives anualitats de contracte es facturarà l'import corresponent a la capacitat contractada.

Els imports es determinaran un cop aplicada la baixa licitatòria oferta per l'adjudicatari.

L'abonament d'aquestes factures queda condicionada a que l'adjudicatari hagi lliurat, actualitzat, el document MS Excel® tal com s'indica en el punt 3.2 del present plec de prescripcions tècniques.

Als anteriors imports s'aplicarà la corresponen baixa licitatòria.

7.2. PER LA IMPLANTACIÓ I GOVERN DE LA PLATAFORMA.

La facturació d'aquesta part del contracte es realitzarà de manera trimestral al llarg del contracte. Aquestes son les fites de facturació:

7.2.1. Activació, Planificació i Fundació

Fita 1: Activació de la plataforma i connectivitat resilient (finalitzat el 1r trimestre – 8 % de l'import d'adjudicació corresponent a la implantació i govern)

Activar la plataforma Low Code i garantir que totes les funcionalitats bàsiques estiguin operatives.

Establir una **connectivitat segura i resilient i amb suficient capacitat** entre el IMI i la plataforma (incloent redundància i monitoratge). Aquesta tasca inclou totes les configuracions i desenvolupaments necessaris fins validar que les crides des de l'origen arriben al API Manager Corporatiu.

Configurar l'entorn inicial amb les eines necessàries per desenvolupar i operar.

Fita 2: Definició de l'estratègia i programa d'adopció (finalitzat el 2n trimestre – 8 % de l'import d'adjudicació corresponent a la implantació i govern)

Crear les línies estratègiques per a l'adopció de la tecnologia.

Desenvolupar els mecanismes de mesura de resultats.



Fita 3: Creació de processos de gestió de la demanda (finalitzat el 3r trimestre– 8 % de l'import d'adjudicació corresponent a la implantació i govern)

Establir el procediment per prioritzar iniciatives segons el ROI i riscos.
Alinear les iniciatives amb el volum de subministraments subscrites.

Fita 4: Adopció de la metodologia de desenvolupament del fabricant (finalitzat el 4rt trimestre– 8 % de l'import d'adjudicació corresponent a la implantació i govern)

Analitzar i adaptar la metodologia del fabricant a les necessitats organitzatives.
Publicar una guia interna per als equips.

Fita 5: Inici de la gestió del canvi organitzacional (finalitzat el 5è trimestre– 8 % de l'import d'adjudicació corresponent a la implantació i govern o import restant de l'actualitat si aquest es menor)

Formar i sensibilitzar els equips sobre la nova tecnologia.
Introduir material de formació com píndoles i documentació tècnica.

7.2.2. Implementació i Operació Inicial

Fita 6: Implementació i monitoratge de la infraestructura Low Code (finalitzat el 6è trimestre– 8 % de l'import d'adjudicació corresponent a la implantació i govern)

Instal·lar components bàsics i establir protocols de monitoratge.
Garantir la gestió de permisos i l'estabilitat inicial.

Fita 7: Garantir l'alineació amb arquitectura, seguretat i qualitat (finalitzat el 7è trimestre– 8 % de l'import d'adjudicació corresponent a la implantació i govern)

Validar diagrames d'arquitectura amb els arquitectes.
Documentar processos de seguretat i arquitectura.

Fita 8: Llançament de components reutilitzables (finalitzat el 8è trimestre– 8 % de l'import d'adjudicació corresponent a la implantació i govern)

Desenvolupar i publicar els primers components reutilitzables.
Establir una biblioteca centralitzada per a la seva distribució.

Fita 9: Primer cicle de millora contínua (finalitzat el 9è trimestre– 8 % de l'import d'adjudicació corresponent a la implantació i govern o import restant de l'actualitat si aquest es menor)

Implementar un pipeline inicial DevOps.
Realitzar sessions de feedback amb els equips de desenvolupament.

7.2.3. Maduració i Optimització

Fita 10: Ampliació de les funcionalitats i suport avançat (finalitzat el 10è trimestre– 8 % de l'import d'adjudicació corresponent a la implantació i govern)

Desplegar funcionalitats de CI/CD per a entorns productius.



Fer proves avançades de càrrega, estrès i seguretat.

Fita 11: Maximització del reaprofitament de components (finalitzat l'11è trimestre– 8 % de l'import d'adjudicació corresponent a la implantació i govern)

Optimitzar components existents i desenvolupar-ne de nous.
Consolidar l'ús de components en tota l'organització.

Fita 12: Aprofundiment en la millora contínua i formació i estabilització i revisió del govern de la plataforma (finalitzat el 12è trimestre– 12 % de l'import d'adjudicació corresponent a la implantació i govern)

Refinar la qualitat del codi i dels desenvolupaments.
Avaluar l'eficàcia dels processos implementats.
Realitzar ajustos segons les lliçons apreses.
Presentar un pla de manteniment a llarg termini.

Als anteriors imports s'aplicarà la corresponen baixa licitatòria.

8. PROPOSTA TÈCNICA I ECONÒMICA

Es presentaran dos sobres, sobre electrònic B i sobre electrònic C.

Tots els arxius inclosos a cadascun dels sobres electrònics hauran d'estar degudament signats amb signatura electrònica reconeguda de l'empresa licitadora, vàlidament emesa per un Prestador de Serveis de Certificació que garanteixi la identitat i integritat dels documents, de conformitat amb el que estableix la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança, i la resta de disposicions de contractació pública electrònica.

A continuació, es descriuen els continguts de cadascun dels sobres.

8.1. CONTINGUT DEL SOBRE ELECTRÒNIC B

En el sobre electrònic B les empreses licitadores presentaran la seva oferta tècnica de realització del contracte tant per fer comprensible la seva proposta com per facilitar i fer possible la seva valoració d'acord amb els criteris d'adjudicació assenyalats en el plec de clàusules administratives particulars que regeixen aquesta contractació.

Les empreses licitadores hauran de presentar la seva oferta en format electrònic degudament signat per l'empresa licitadora o persona que la representi, a través de la plataforma electrònica de licitació de l'Ajuntament de Barcelona: <https://licitacions.bcn.cat/>. A l'oferta tots els arxius han d'estar en format **Open Document (odt o odp) o pdf obligatori**, en format no protegit, amb fonts incrustades i que accepti cerques, seleccions i copiat del text.

S'inclourà la següent documentació, si s'escau, indexada i numerada de manera que faciliti la seva localització:



Proposta tècnica:

Les empreses licitadores inclouran la seva proposta tècnica en un únic arxiu, a tipus de lletra Nimbus Roman, Liberation Sans, Calibri, Arial, Times New Roman o similar, de grandària 11 i interlineat simple.

A nivell general i d'aplicació a tota la proposta tècnica, es valorarà a partir de l'alineació de la plataforma amb les necessitats estratègiques i operatives de l'organització, la competència del licitant i l'enteniment del plec tècnic i de l'abast. No es tindrà en consideració la còpia directa d'elements o apartats del plec tècnic, i es requereix que sigui específic per l'objecte del contracte i pels requeriments descrits al plec tècnic.

La proposta tècnica haurà de contenir i seguir obligatòriament l'ordre dels següents punts:

1. Plantejament general

S'exposa l'enteniment del contracte amb una breu introducció de la plataforma proposada i el servei que s'ha de prestar i les línies principals de l'estratègia per dur-lo a terme i l'esquema de l'equip del treball indicant i la seva organització, tenint en compte els requeriments exposats en el plec de prescripcions tècniques. Inclourà un resum executiu de la proposta amb els esquemes i aspectes clau que es considerin.

2. Proposta Específica

Ha d'incloure la descripció que millor demostrï les característiques a valorar de les **àrees avaluables amb criteris tècnics subjectes a judici de valor:**

- a. Arquitectura
N aspectes i característiques a valorar(*)
- b. Facilitat d'ús
N aspectes i característiques a valorar(*)
- c. Capacitats de Desenvolupament i ALM
N aspectes i característiques a valorar(*)
- d. Continuitat del Servei
N aspectes i característiques a valorar(*)
- e. Analítica i Monitorització



N aspectes i característiques a valorar(*)

f. Funcionalitats avançades

N aspectes i característiques a valorar(*)

(*)El plec administratiu detalla els N aspectes i característiques a valorar dins de cada àrea.

També s'inclourà la documentació que s'especifica en el plec de clàusules administratives particulars.

8.2. CONTINGUT SOBRE ELECTRÒNIC C

En el **sobre electrònic C** s'inclourà l'oferta econòmica i aquella documentació que haurà de ser valorada segons els criteris avaluable de forma automàtica, assenyalats en les clàusules del plec de clàusules administratives particulars que regeixen per aquesta contractació, així com qualssevol altra documentació que aquest estableixi..

9. CLAUSULES GENERALS DE SEGURETAT

9.1. SEGURETAT DELS SISTEMES D'INFORMACIÓ, PROTECCIÓ DE DADES I COMPLIMENT NORMATIU

L'IMI ha adoptat com a marc de referència per a la Seguretat dels Sistemes d'Informació el conjunt de bones pràctiques internacionalment reconegudes que desenvolupa la norma ISO-27002:2013.

L'IMI, com a Organisme Autònom de caràcter administratiu de l'Administració Local depenent de l'Ajuntament de Barcelona, es troba subjecte al Principi de Legalitat i posa especial èmfasi en el compliment de les obligacions legals que es deriven de la Llei Orgànica 3/2018 de Protecció de Dades Personals i Garantia de Drets Digitals, de la Llei 39/2015 en tot allò que fa referència a l'accés dels ciutadans als serveis públics, així com de la resta de l'ordenament jurídic que sigui d'aplicació.

Pel què fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació, es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el RD 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat.

Les empreses licitadores s'obliguen a vetllar pel compliment de la legislació vigent aplicable a l'objecte del contracte i especialment pel què fa referència a la protecció de dades de caràcter personal.

A les diferents clàusules d'aquesta secció es fa referència a Ajuntament de Barcelona, Administració Municipal i IMI indistintament. De conformitat als seus estatuts s'ha d'entendre que l'IMI actua als efectes d'aquest contracte en nom i representació de l'Ajuntament de Barcelona i de l'Administració Municipal, pel que fa referència als fitxers, sistemes d'informació i/o infraestructures de les que no sigui directament titular.



9.2. CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT

Pel què fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació, es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el RD 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat (en endavant ENS).

Donada la naturalesa del contracte, l'adjudicatari haurà de donar compliment als requeriments establerts a l'ENS pel MIG.

D'igual manera per qualsevol obligació legal que recaigui en l'Ajuntament, el proveïdor haurà de donar compliment per la part que li correspongui segons l'abast del contracte.

L'adjudicatari haurà d'acreditar la conformitat amb l'ENS mitjançant alguna de les següents opcions:

- Certificació oficial d'una entitat de certificació acreditada.
- Informe d'auditoria de compliment. L'adjudicatari serà responsable de disposar d'un informe d'auditoria (en el que l'ENS formi part del seu abast) de compliment on es detalli que els productes de seguretat, equips, sistemes i aplicacions compleixen amb totes les mesures aplicables de l'Esquema Nacional de Seguretat.

L'adjudicatari garantirà l'accés per part de l'IMI a auditar tota la informació necessària per donar compliment a aquestes regulacions (procediments, anàlisi de riscos, registre d'incidents, pla d'adequació, etc.).

D'igual manera, en el cas que es subcontracti, totalment o parcial, els subministraments i serveis associats objecte del present contracte, les empreses subcontractades quedaran a totes les mesures de seguretat d'aplicació a l'adjudicatari dins de l'abast dels servis subcontractats. És responsabilitat de l'adjudicatari assegurar-se que l'empresa subcontractada compleix amb el nivell de l'ENS corresponent, així com amb el conjunt de mesures de seguretat determinades en aquest clausulat de seguretat.

9.3. CLÀUSULA DE PROPIETAT INTEL·LECTUAL

Tot i reconeixent l'autoria de les persones que els hagin elaborat, la propietat intel·lectual dels treballs realitzats a l'empareda d'aquest contracte pertany a l'Ajuntament de Barcelona de forma exclusiva. Els productes o subproductes derivats, no podran ser utilitzats sense la deguda autorització prèvia.

L'accés a informació i/o productes protegits per la propietat intel·lectual, propietat de l'Ajuntament de Barcelona, necessaris per al desenvolupament del producte o servei contractat no pressuposa en cap cas la cessió de la mateixa ni es permet el seu ús sense autorització expressa d'aquest ajuntament.

L'empresa contractada accepta expressament que els drets d'explotació dels productes derivats d'aquest plec corresponen única i exclusivament a l'Ajuntament de Barcelona. Així doncs, el contractat cedeix, amb caràcter d'exclusivitat, la totalitat dels drets d'explotació dels treballs objecte d'aquest plec, inclosos els drets de comunicació pública, reproducció,



transformació o modificació i qualsevol d'altre dret susceptible de cessió en exclusiva, d'acord amb la legislació sobre drets de propietat intel·lectual.

9.4. CLÀUSULA PER ACCESSOS POTENCIALS

L'adjudicatari, tot i que pel desenvolupament de les seves funcions no té accés a dades de caràcter personals, pot tenir-hi un accés potencial o accidental.

En aquesta contractació no es preveu tractament de dades personals per part de l'empresa contractista.

Per a l'execució de les prestacions derivades del compliment de l'objecte d'aquest contracte, el personal de l'empresa contractista no pot accedir a les dades de caràcter personal que figuren als arxius, documents i sistemes informàtics de l'òrgan de contractació.

No obstant el que estableix el paràgraf anterior, quan el personal de l'empresa contractista accedeixi a les dades personals incidentalment, estarà obligat a guardar secret fins i tot després de la finalització de la relació contractual, sense que en cap cas pugui utilitzar les dades ni revelar-les a tercers.

L'empresa contractista ha de posar en coneixement dels seus treballadors els deures i obligacions establerts anteriorment.

L'empresa contractista ha de posar en coneixement de l'òrgan de contractació, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de les dades de caràcter personal. Aquesta incidència s'haurà d'anotar al Registre d'incidències.

L'incompliment del que s'estableix en els apartats anteriors pot donar lloc a l'empresa contractista sigui considerada responsable del tractament, als efectes d'aplicar el règim sancionador i de responsabilitats previst a la normativa de protecció de dades.

9.5. CONFIDENCIALITAT

L'adjudicatari s'obliga a no difondre i a guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del present contracte i a subministrar-la només al personal autoritzat per l'Ajuntament.

L'adjudicatari queda expressament obligat a mantenir absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer com a conseqüència de la participació en la present licitació, o, amb ocasió del compliment del contracte, especialment els de caràcter personal, que no podran copiar o utilitzar com a finalitat diferent a les que la informació te designada.

Quan l'objecte del contracte sigui la construcció i/o el manteniment de Sistemes d'Informació i/o Infraestructures Tecnològiques, el deure de secret inclou els components tecnològics i mesures de seguretat tècniques implantades en els mateixos.

L'adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal al seu càrrec. Així mateix, s'obliga a aplicar les mesures necessàries per a garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal participant en el desenvolupament del contracte.



Un cop finalitzat el present contracte, l'adjudicatari es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per l'Ajuntament, així com qualsevol altre producte obtingut com a resultat del present contracte.

10. CLÀUSULES IMPLANTACIÓ D'UN PRODUCTE

10.1. GESTIÓ D'IDENTITATS, AUTENTICACIÓ D'USUARIS

La gestió d'identitats dels usuaris del sistema haurà de complir les polítiques d'usuaris, administradors i contrasenyes definides per l'IMI les quals es troben a disposició dels sol·licitants.

L'empresa proveïdora haurà de validar i revisar accessos dels usuaris i perfils administradors de forma semestral, i haurà d'establir i implementar els plans d'acció per corregir les mancances identificades. Els comptes d'usuari estaran integrats amb l'eina que l'IMI posa a disposició.

Autenticació interna: Els usuaris interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per l'IMI basats en protocols estàndards de seguretat. L'empresa proveïdora haurà d'assegurar que s'utilitzi el proveïdor d'identitats corporatiu (en endavant, IDP) per a l'autenticació dels usuaris.

La integració amb la solució IDP es podrà fer mitjançant les següents opcions:

- Integració mitjançant l'estàndard OpenID Connect (OAuth 2.0), utilitzant el flux d'autenticació de codi d'autorització amb PKCE (intercanvi de clau codificada)
- En cas de que l'aplicació no suporti l'ús del protocol OpenID Connect, la integració es farà mitjançant l'estàndard SAML 2.0.

Autenticació externa: Els usuaris externs (fora de l'àmbit municipal, empreses i altres persones físiques - clients de l'aplicació) hauran d'autenticar-se mitjançant la solució corporativa (Mòdul Comú d'Autenticació).

L'autenticació al sistema s'haurà de produir amb un segon factor d'autenticació (2FA), requerint així una verificació de la identitat de l'usuari que sol·licita accés. L'adjudicatari aplicarà el mateix 2FA que sigui d'aplicació a l'Ajuntament i, en cas de no ser possible haurà de justificar aquesta impossibilitat tècnica, tot aplicant un 2FA diferent que haurà de ser validat per l'IMI.

10.2. AUTORITZACIÓ DELS USUARIS ALS SISTEMES

L'IMI disposa d'un repositori centralitzat d'autoritzacions dels usuaris corporatius, basat en un directori actiu, que és d'on recull les autoritzacions el IDP corporatiu. L'adjudicatari haurà d'assegurar que les autoritzacions es troben delegades en aquest repositori central d'autoritzacions.

En cas que l'adjudicatari no pugui delegar l'autorització per impediments greus del sistema, com a mínim, hauran d'integrar-se amb l'eina de gestió i govern de les identitats per tal de poder relacionar els rols del producte (tècnica de sistemes) amb els rols funcionals definits a GID (capa de negoci).

Aquesta integració podrà ser de dos tipus:



- Integració directa amb la GID, si l'aplicació pot publicar els usuaris i perfils a través d'un servei web que es pugui consumir mitjançant un connector des de l'eina de gestió d'identitats.
- En cas de no ser possible la connexió directa amb la GID, l'aplicació haurà d'enviar un fitxer diari a la GID i configurar un connector de processament de fitxers per tal de representar les autoritzacions a l'eina.

La integració d'aquest connector anirà a càrrec de l'empresa adjudicatària i comptarà amb el suport i la supervisió de l'equip de gestió d'identitats.

Perfilat d'usuaris: Les autoritzacions han de seguir un model RBAC (Role Based Access Control) que haurà de ser validat pels responsables tecnològics de la plataforma i pel Departament de Seguretat de l'IMI.

El model proposat haurà de complir amb els següents principis:

- Segregació de funcions, de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.
- Mínim privilegi, els privilegis de cada usuari es reduiran al mínim estrictament necessari per complir les seves obligacions.
- Necessitat de Conèixer, els privilegis es limitaran de manera que els usuaris només accediran al coneixement d'aquella informació requerida per complir les seves obligacions.
- Capacitat d'autorització, només i exclusivament el personal amb competència d'autorització, podrà concedir, alterar o anul·lar l'autorització d'accés als recursos, conforme als criteris establerts pel seu responsable.
- La gestió de permisos haurà de ser en base a perfils i rols, podent un usuari tenir múltiples perfils. Els usuaris només podran accedir a aquelles funcions que tinguin expressament autoritzades. La implementació ha de permetre la implementació de matrius de segregació de funcions i l'agilitat en l'administració d'aquests permisos.

Per facilitar l'administració s'hauran de poder gestionar els permisos mitjançant rols de seguretat, entenent com a rol una entitat que dona accés a una sèrie d'operacions.

Sota la premissa d'aquests criteris generals, l'adjudicatari haurà de dissenyar el joc de permisos i autoritzacions requerits pels sistemes d'informació implementats, en base al document 'Pla d'Autoritzacions'. Aquest document serà revisat i actualitzat per l'adjudicatari per incloure nous punts a tractar o adaptacions dels punts existents.

10.3. PROTECCIÓ DE LES APLICACIONS I SERVEIS WEB

L'adjudicatari garantirà que els subsistemes dedicats a la publicació de la informació hauran de ser protegits front a les amenaces que li siguin pròpies:



- Quan la informació tingui algun tipus de control d'accés, es garantirà la impossibilitat d'accedir a la informació obviant l'autenticació, en concret prenent mesures en els següents aspectes:
 - S'evitarà que el servidor ofereixi accés a documents per vies alternatives al protocol determinat.
 - Es previndran atacs de manipulació de URL.
 - Es previndran atacs de manipulació de fragments de la informació que s'emmagatzemin en el disc dur del visitant d'una pagina web a través del seu navegador, a petició del servidor de la pagina, conegut en la terminologia anglesa com a "cookies".
 - Es previndran atacs d'injecció de codi.
- Es previndran intents d'escalat de privilegis.
- Es previndran atacs de "cross site scripting".
- Es faran servir certificats d'autenticació de llocs web d'acord amb les polítiques establertes per la Direcció de Serveis de Seguretat de la Informació.

10.4. ACCEPTACIÓ I POSTA EN SERVEI

L'adjudicatari ha de comprovar el correcte funcionament de l'aplicació, per tal de garantir que:

- Es compleixen els criteris d'acceptació en la matèria de seguretat.
- No es deteriora la seguretat d'altres components del servei.

Adicionalment per al nivell mitjà, l'adjudicatari realitzarà les següents inspeccions prèvies a l'entrada en servei:

- Anàlisi de vulnerabilitats.
- Test de penetració.

10.5. DADES DE PROVES

L'adjudicatari es compromet a assumir tota la responsabilitat en la creació de dades de proves per testejar els serveis. En cap cas s'utilitzaran dades de l'entorn de producció per fer proves.

En cas que sigui necessari copiar dades de l'entorn productiu, aquestes seran les mínimes necessàries i hauran de ser sotmeses a un procés d'ofuscació. L'adjudicatari es farà càrrec del desenvolupament dels procediments de tractament de dades (ofuscació, truncament, etc.) en cas que fossin necessaris.

Tota manipulació de dades de l'entorn de producció haurà de ser informada i aprovada pel propietari de les mateixes.

En cas que s'hagi de realitzar una migració de dades entre sistemes, l'adjudicatari haurà de presentar un pla de migració de les dades on es detallin les operacions necessàries.



Aquest pla de migració s'adequarà al procediment establert per seguretat per tal de minimitzar l'exposició de les dades productives.

10.6. XIFRATGE DE DADES

Qualsevol informació corporativa que requereixi ser xifrada en la seva ubicació d'emmagatzemament (i per tant, queda exclòs l'encriptació per transit en les comunicacions) ha de seguir els estàndards de seguretat, custòdia i protecció de les claus que estableix la Direcció de Serveis de Seguretat de la Informació per tal d'assegurar la disponibilitat de la informació als propietaris d'aquesta dins de l'Ajuntament. La Direcció de Serveis de Seguretat de la Informació custodiarà les claus de xifratge.

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents amb la informació municipal o corporativa, el proveïdor haurà de presentar-les per ser validades per la Direcció de Serveis de Seguretat de la Informació i/o seguir els estàndards i normes de l'IMI.

10.7. SIGNATURA ELECTRÒNICA

Qualsevol requeriment de signatures digitals que s'hagin de produir referents amb la informació municipal o corporativa, el proveïdor haurà de presentar-les per ser validades per la Direcció de Serveis de Seguretat de la Informació i/o seguir els estàndards i normes de l'IMI.

Per la signatura electrònica s'empraran els mecanismes aprovats per l'IMI, en cas que hagin de ser uns altres, s'haurà de justificar, documentar tècnicament i haurà d'estar validat per la Direcció de Serveis de Seguretat de la Informació. En tot cas s'ha de complir la política de signatura electrònica de l'ajuntament de Barcelona.

10.8. CERTIFICATS

La Direcció de Serveis de Seguretat de la Informació serà el responsable de la custòdia i protecció dels certificats digitals emesos en nom de l'Ajuntament de Barcelona a través de la Direcció de Serveis de Seguretat de la Informació. S'entén per certificats digitals corporatius: els de servidor segur, els d'aplicatiu per autenticació o signatura digital, de signatura de codi, de xifratge, etc.

Tots els certificats hauran de ser sol·licitats a través del procediment establert en la Direcció de Serveis de Seguretat de la Informació per al seu control i gestió.

El proveïdor haurà de seguir l'estàndard establert per la protecció i custòdia dels certificats digitals a l'hora d'incorporar el certificat pel seu ús.

10.9. PLA DE TRACES

Les aplicacions o productes que permeten realitzar operacions sobre les dades de negoci han de proporcionar informació sobre les accions i accessos realitzats en aquesta informació. Tant la criticitat de les dades i els criteris del negoci, com els requeriments legals marcaran la informació que cal recollir i el temps de retenció dels logs.



L'adjudicatari haurà de configurar el sistema per recollir les traces necessàries en base al Document del 'Pla de Seguretat i Traces' que posarà a disposició l'IMI a l'inici del contracte. Dins d'aquest registre, s'ha d'incloure:

- Qui realitza l'activitat (tant usuaris com operadors i administradors en especial), quan i el sistema en qüestió.
- Registre d'activitats realitzades amb èxit i les rebutjades.
- Les activitats concretes subjectes a ésser registrades vindran determinades per l'anàlisi de riscos del sistema.

Un cop configurades les traces s'hauran d'incorporar en els documents estàndards de seguretat: 'Pla mestre de Traces' (on s'avaluen els requeriments de les traces, el disseny i es determina l'inventari de traces necessàries) en la fase d'anàlisi i el document 'Pla de Traces' (on s'aporten detalls i mostres de cadascuna de les traces) en fase de proves i/o pas a producció

11. CLÀUSULES ADMINISTRACIÓ

11.1. INVENTARI D'ACTIUS

L'adjudicatari haurà de mantenir un inventari actualitzat de tots els elements del sistema, detallant la seva naturalesa i identificant al seu responsable; és a dir, la persona que és responsable de les decisions relatives al mateix.

11.2. CONFIGURACIÓ DE SEGURETAT

L'adjudicatari haurà de configurar els equips prèviament a la seva entrada en operació, de manera que:

- Es retirin comptes i contrasenyes estàndard.
- S'aplicarà la regla de "mínima funcionalitat":
 - El sistema ha de proporcionar la funcionalitat requerida perquè l'organització aconsegueixi els seus objectius i cap altra funcionalitat.
 - No proporcionarà funcions gratuïtes, ni d'operació, ni d'administració, ni d'auditoria, reduint d'aquesta forma el seu perímetre al mínim imprescindible.
 - S'eliminarà o desactivarà mitjançant el control de la configuració, aquelles funcions que no siguin d'interès, no siguin necessàries, i fins i tot, aquelles que siguin inadequades al fi que es persegueix.
- S'aplicarà la regla de "seguretat per defecte":
 - Les mesures de seguretat seran respectuoses amb l'usuari i protegiran a aquest, tret que s'exposi conscientment a un risc.
 - Per reduir la seguretat, l'usuari ha de realitzar accions conscients.
 - L'ús natural, en els casos que l'usuari no ha consultat el manual, serà un ús segur.



11.3. MANTENIMENT

L'adjudicatari haurà de mantenir l'equipament físic i lògic que constitueix el sistema i/o infraestructura administrada.

L'adjudicatari haurà de mantenir actualitzats els productes utilitzats en l'abast del plec d'acord a la política acordada amb l'IMI.

La política d'actualitzacions està basada en el nivell de criticitat de la vulnerabilitat valorada segons l'última versió publicada de l'estàndard públic CVSS (Common Vulnerability Scoring System), segons el nivell de CVSS les actualitzacions per la correcció de vulnerabilitats s'hauran de produir dins d'uns terminis específics (en funció del nivell d'exposició, la criticitat de la vulnerabilitat i la criticitat de l'actiu afectat), detallats en la taula següent:

		Nivell d'exposició			
		Exposat a internet		No exposat a internet	
		Criticitat de l'actiu		Criticitat de l'actiu	
		Crític	No crític	Crític	No crític
Criticitat vulnerabilitat	CVSS <=3	20 dies	40 dies	40 dies	40 dies
	3 < CVSS <= 6	5 dies	1 mes	20 dies	20 dies
	6 < CVSS <=8	1 dia	5 dies	5 dies	5 dies
	CVSS > 8	1 dia	2 dies	1 dia	5 dies

El proveïdor s'haurà d'involucrar en tot el cicle de vida de les vulnerabilitats, des de la seva detecció fins a la mitigació d'aquesta. Haurà de tenir un seguiment proactiu de les vulnerabilitats que es puguin produir amb un seguiment continu del anunci de defectes, mantenint el contacte amb els fabricants per tenir coneixement de les possibles solucions que aquest proposin per corregir-les.

11.4. ANTIMALWARE

L'adjudicatari serà responsable de la instal·lació i actualització de programes de protecció antimalware de les màquines que suporten serveis de l'IMI segons es recull al marc normatiu del l'IMI.

L'IMI obtindrà indicadors de la bona gestió de proteccions antimalware i en qualsevol moment tindrà accés i visió de l'estat de la seguretat global de les proteccions.

La Direcció de Seguretat de la Informació de l'IMI tindrà accés en consulta a la consola de gestió d'aquests programaris del proveïdor.



11.5. CÒPIES DE SEGURETAT

L'adjudicatari serà responsable de realitzar còpies de seguretat als sistemes dels quals és administrador per tal de poder recuperar les dades en cas de pèrdua accidental o intencionada. La freqüència de les còpies de seguretat vindrà donada pel nivell de sensibilitat de les dades que conté, segons el recollit a les guies de l'IMI.

El nivell de seguretat d'aquestes dades ha de ser un reflex del de les dades originals a tots els nivells (integritat, confidencialitat, autenticitat y traçabilitat). Per tal de garantir la confidencialitat, l'IMI es reserva el dret de demanar el xifrat de les dades. L'abast de les còpies inclou:

- Informació de treball de l'IMI.
- Aplicacions en explotació, incloent els sistemes operatius.
- Dades de configuració, serveis, aplicacions, equips o d'altres anàlegs.
- Claus emprades per conservar la confidencialitat de la informació.

11.6. CONTROL D'ACCÉS

11.6.1. Segregació de funcions i tasques

L'adjudicatari s'encarregarà de que el sistema de control d'accés s'organitzi de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.

En concret, se separaran almenys les següents funcions:

- Desenvolupament d'operació. Garantint, com a mínim, que els desenvolupadors únicament disposin d'accés a l'entorn de preproducció i desenvolupament. La configuració dels entorns productius l'haurà de realitzar persones o equips diferents.
- Configuració i manteniment del sistema d'operació.
- Auditoria o supervisió de qualsevol altra funció.

11.7. EXPLOTACIÓ

11.7.1. Gestió de la configuració

L'adjudicatari s'encarregarà de gestionar de forma continua la configuració dels components del sistema de manera que:

- Es mantingui a tot moment la regla de "funcionalitat mínima".
- Es mantingui a tot moment la regla de "seguretat per defecte".
- El sistema s'adapti a les noves necessitats, prèviament autoritzades.
- El sistema reaccioni a vulnerabilitats reportades.
- El sistema reaccioni a incidents.



11.7.2. Gestió de canvis

L'adjudicatari s'encarregarà de mantenir un control continu de canvis realitzats en el sistema, de manera que:

- Tots els canvis anunciats pel fabricant o proveïdor seran analitzats per determinar la seva conveniència per ser incorporats, o no.
- Abans de posar en producció una nova versió o una versió amb un pegat, es comprovarà en un equip que no estigui en producció, que la nova instal·lació funciona correctament i no disminueix l'eficàcia de les funcions necessàries per al treball diari. L'equip de proves serà equivalent al de producció en els aspectes que es comproven.
- Els canvis es planificaran per reduir l'impacte sobre la prestació dels serveis afectats.
- Mitjançant anàlisi de riscos es determinarà si els canvis són rellevants per a la seguretat del sistema. Aquells canvis que impliquin una situació de risc de nivell alt seran aprovats explícitament de forma prèvia a la seva implantació.

11.7.3. Protecció de claus criptogràfiques

- L'adjudicatari utilitzarà programes avaluats o dispositius criptogràfics certificats.
- S'empraran algoritmes acreditats pel "Centre Criptològic Nacional".

11.8. PROTECCIÓ DELS SERVEIS

11.8.1. Protecció enfront de la denegació de servei

L'adjudicatari establirà mesures preventives i reactives enfront d'atacs de denegació de servei (DoS Denial of Service). Per tal de garantir-ho:

- Es planificarà i dotarà al sistema de capacitat suficient per atendre a la càrrega prevista sense posar en risc la disponibilitat del sistema.
- Es desplegaran tecnologies per prevenir els atacs coneguts.

Barcelona,

Ivan Ortiz Quintana
Cap del Departament d'Arquitectura de
Sistemes d'Informació i Solucions

Jose A. Tórtola Fernandez
Director de Serveis de Desenvolupament



12. ANNEXOS

12.1. ANNEX 1. RELACIÓ DE SUBMINISTRAMENTS DEL PRODUCTE LOW CODE

La subscripció de la plataforma en quant al seu dimensionament haurà d'incloure necessàriament com a mínim els següents conceptes, tenint en compte que les aplicacions es mesuraran en base a la seva complexitat, fent servir el concepte AO:

AOS
Usuaris identificats interns de l'Organització
Usuaris no identificats, externs a l'Organització

En aquesta licitació no es limita el nombre exacte d'aplicacions que es poden desenvolupar i utilitzar. Aquest nombre vindrà determinat per la complexitat d'aquestes.

Amb les capacitats que detallem a continuació fem la següent estimació d'aplicacions a posar en marxa:

Definició de Talles:

Talles	Elements per aplicació				TOTAL
	Pantalles	Taules	Serveis / Integracions	Altres Elements	
Petita	5	20	5	5	35
Mitjana	15	30	10	15	70
Gran	30	60	15	25	130
XL	60	120	30	50	260

Escenari orientatiu de posades en producció d'aplicacions:

Talles	Any1	Any2	Any3
Petita	5	10	15
Mitjana	0	3	6
Gran	0	1	2
XL		0	1
TOTAL ACUMULAT	5	14	24

Durant la vigència del contracte es preveu desenvolupar 24 aplicacions de diferent complexitat.

Un objecte d'aplicació (AO) és una mesura de la complexitat de les aplicacions a la plataforma Low Code. Cada pantalla, taula d'entitat/base de dades, mètode d'API i esdeveniment



automàtic ((acció asíncrona de back-end que es pot disparar de forma automàtica sota determinades condicions) personalitzat de les aplicacions compten com a 1 AO).

Els usuaris podran accedir indistintament a totes les aplicacions existents.

S'ha utilitzat el concepte d'usuari identificat en ser un concepte pràcticament universal, però es vol contractar i facturar segons el nombre d'usuaris actius.

Els usuaris actius podran accedir indistintament a cada una de les aplicacions existents.

Els usuaris actius són aquells usuaris identificats (els usuaris que accedeixen públicament, és a dir sense identificar, a aplicacions que no ho necessiten, no comptabilitzen als còmputos d'usuaris a contractat) únics (diferents) que interactuen amb la plataforma durant el període de 24 hores. D'aquesta manera, en cada període de 24 hores mai no es podrà superar el límit d'usuaris actius contractats. En tot cas, mai no es contractarà per usuaris nominals, és a dir, usuaris que poden tenir la capacitat d'interactuar amb la plataforma.

S'entén com a usuari identificat intern de l'organització tots els usuaris identificats a la Gestió d'Identitats (sistema d'identificació i autenticació intern de l'Ajuntament de Barcelona), independentment de la relació laboral amb l'ajuntament de Barcelona. Usuari identificat extern, és aquell usuari que s'identifica perquè les exigències de l'aplicació així ho estableixen, amb algun procés diferent de la gestió d'identitats (certificats, idCAT, @clau,).

Capacitats a licitar:

Anualitat 2025-2026		
Subscripcions	SKU	Quantitat
AOS		150
Usuaris identificats interns de l'Organització		200
Usuaris no identificats, externs a l'Organització		il·limitat

Anualitat 2026-2027		
Subscripcions	SKU	Quantitat
AOS		600
Usuaris identificats interns de l'Organització		500
Usuaris identificats externs a l'Organització		10.000
Usuaris no identificats, externs a l'Organització		il·limitat



Anualitat 2027-2028		
Subscripcions	SKU	Quantitat
AOS		1.800
Usuaris identificats interns de l'Organització		800
Usuaris identificats externs a l'Organització		10.000
Usuaris no identificats, externs a l'Organització		il·limitat

Durant la durada del contracte **aquests volums podran ser ampliat**s. Els tipus de subscripció que han d'estar disponibles per ser ampliat es son:

Possible ampliació per la anualitat 2025-2026		
Subscripcions	SKU	Quantitat
AOS		150
Usuaris identificats interns de l'Organització		0
Usuaris identificats externs a l'Organització		0

Possible ampliació per la anualitat 2026-2027		
Subscripcions	SKU	Quantitat
AOS		150
Usuaris identificats interns de l'Organització		100
Usuaris identificats externs a l'Organització		10.000

Possible ampliació per la anualitat 2027-2028		
Subscripcions	SKU	Quantitat
AOS		300
Usuaris identificats interns de l'Organització		100
Usuaris identificats externs a l'Organització		10.000

L'adquisició de la plataforma es realitzarà per unitats o per packs, tal com s'indica als apartats 3 i 4, i concordants, del present plec.