Barcelona
Institut Municipal d'Informàtica
Direcció de Serveis al Lloc de Treball

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DE LA IMPLANTACIÓ DEL NOU GESTOR D'IDENTITATS DE L'AJUNTAMENT DE BARCELONA, AMB MESURES DE CONTRACTACIÓ PÚBLICA SOSTENIBLE

Contingut

1 INTRODUCCIÓ 4

2 ASPECTES GENERALS DEL CONTRACTE 5

2.1 OBJECTE 5
2.2 ABAST I ÀMBIT DEL CONTRACTE 5

3 SITUACIÓ ACTUAL 6

3.1 ARQUITECTURA 7
3.2 SISTEMES INTEGRATS 7
3.2.1 Núvol de Microsoft 9
3.3 TIPOLOGIA D'IDENTITATS 9
3.4 CICLE DE VIDA DE LES IDENTITATS 9
3.5 SINCRONITZACIÓ DE LA CONTRASENYA 11

4 DESCRIPCIÓ DE LES TASQUES OBJECTE DEL CONTRACTE 12

4.1 GOVERNANÇA DE LES IDENTITATS 12
4.2 GESTIÓ I CONTROL D'IDENTITATS, ACCESSOS, AUTENTICACIONS I AUTORITZACIONS 15
4.3 IMPLANTACIÓ D'UNA NOVA EINA DE GESTIÓ I ADMINISTRACIÓ D'IDENTITATS I ACCESSOS 18
4.3.1 Fase I - Anàlisi inicial del projecte 18
4.3.2 Fase II – Disseny de la solució del projecte 18
4.3.3 Fase III – Desplegament del projecte del nou gestor d'identitats 19
4.3.4 Fase IV – Redefinició i migració de l'actual sistema de gestió d'identitats 20
4.3.5 Fase V – Aturada de la plataforma actual de gestió d'identitats 21
4.4 ADMINISTRACIÓ, OPERACIÓ I EVOLUCIÓ DE LA NOVA EINA DE GESTIÓ D'IDENTITATS 21
4.5 EVOLUTIUS SOBRE LA PLATAFORMA ACTUAL DE GESTIÓ D'IDENTITATS (OIM) 25
4.6 FINALITZACIÓ DEL SERVEI I TRASPÀS DEL SERVEI 25
4.7 PLANIFICACIÓ PROPOSADA 26

5 EQUIP DE TREBALL 27

5.1 FUNCIONS 27
5.2 EXPERIÈNCIA I CONEIXEMENTS 29
5.3 DIMENSIONAMENT 31
5.4 MODEL DE GOVERN 32
5.5 COMITÈ DE SEGUIMENT 32
5.6 COMITÈ DE DIRECCIÓ 33
5.7 COMITÈ DE CRISI 34

6 REQUERIMENTS DE LA NOVA SOLUCIÓ DE GESTIÓ D'IDENTITATS 35

6.1 REQUERIMENTS D'INFRAESTRUCTURA (R.IN.) 35
6.2 REQUISITS DE LA SOLUCIÓ TECNOLÒGICA (R.TE.) 35
6.3 REQUERIMENTS BÀSICS DEL DESPLEGAMENT (R.DE.) 39
6.4 REQUERIMENTS DEL CICLE DE VIDA DE LA IDENTITAT (R.CV.) 39
6.5 REQUISITS D'ADMINISTRACIÓ DELEGADA (R.AD.) 41
6.6 REQUISITS DELS FLUXOS DE PETICIONS (R.FP.) 42
6.7 REQUERIMENTS DE LES CONTRASENYES (R.CO.) 42
6.8 REQUERIMENTS D'INTEGRACIÓ AMB ALTRES SISTEMES (R.IS.) 42

6.9 REQUERIMENTS D'AUDITORIA I INFORMES (R.AI.) 43
6.10 REQUERIMENTS DE COMPLIMENT (R.CU). 44

7 ACORDS DE NIVELL DE SERVEI / COMPLIMENT DE FITES 44

7.1 COMPLIMENT DE FITES DEL PROJECTE D'IMPLANTACIÓ/MIGRACIÓ 44
7.2 OPERACIÓ I ADMINISTRACIÓ DE LA NOVA EINA DE GESTIÓ D'IDENTITATS I ACCESSOS 45
7.2.1 Temps de resposta i resolució d'incidències 46
7.2.2 Temps de resposta PETICIONS DE SERVEI I ACTUALITZACIÓ DE PROBLEMES 46
7.2.3 Reobertura de tiquets 47

8 DOCUMENTACIÓ TÈCNICA I ECONÒMICA DE L'OFERTA I FACTURACIÓ 48

8.1 PROPOSTA TÈCNICA (CONTINGUT SOBRE ELECTRÒNIC B) 48
8.2 PROPOSTA ECONÒMICA (CONTINGUT SOBRE ELECTRÒNIC C) 49
8.3 FACTURACIÓ 49

9 CLÀUSULES GENERALS 51

9.1 ACREDITACIONS I ACCEPTACIÓ DE CONDICIONS I REQUERIMENTS 51
9.2 COMPLIMENT DELS PROCEDIMENTS I ESTÀNDARDS DE L'IMI I GESTIÓ DEL CANVI 51
9.3 LOCALITZACIÓ DE LA PRESTACIÓ DELS SERVEIS I DE L'EQUIP DE PROJECTE 51
9.4 LLENGUA 52
9.5 HORARIS 52
9.6 PERÍODE DE GARANTIA DEL CONTRACTE 52
9.7 CLÀUSULA DE GESTIÓ DE SERVEIS TIC 53

10 CLÀUSULES GENERALS DE SEGURETAT 54

10.1 SEGURETAT DELS SISTEMES D'INFORMACIÓ, PROTECCIÓ DE DADES I COMPLIMENT NORMATIU 54
10.2 CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT (ENS) 54
10.3 RESPONSABLE DE SEGURETAT 55
10.4 DELEGAT DE PROTECCIÓ DE DADES 55
10.5 CLÀUSULA DE PROPIETAT INTEL·LECTUAL 55
10.6 PROTECCIÓ DE DADES DE CARÀCTER PERSONAL 56
10.7 CONFIDENCIALITAT 56
10.8 CLÀUSULA SOFTWARE I METODOLOGIA DE DESENVOLUPAMENT 56
10.9 AUDITORIA 57
10.10 GESTIÓ D'INCIDENTS 58
10.11 ACCÉS A LA INFORMACIÓ 58
10.12 DIMENSIONAMENT I GESTIÓ DE CAPACITATS 58
10.13 ANÀLISISI FORENSES 58
10.14 CONTROL D'ACCÉS 58
10.14.1 Accés local 58
10.14.2 Accés remot 59
10.14.3 Segregació de funcions i tasques 59
10.15 GESTIÓ DEL PERSONAL 59
10.15.1 Deures i obligacions del personal 59
10.15.2 Formació i conscienciació 60
10.16 PROTECCIÓ DEL LLOC DE TREBALL 60
10.16.1 Lloc de treball buit 60
10.16.2 Protecció d'equips 60
10.17 CLÀUSULA DE COMUNICACIONS EXTERNES 61
10.18 PROTECCIÓ DELS SUPORTS INFORMÀTICS 61

10.18.1 Etiquetat *61*
10.18.2 Transport *61*
10.18.3 Esborrat i destrucció *61*
10.19 PROTECCIÓ DE LA INFORMACIÓ 62
10.19.1 Neteja de documents *62*
10.19.2 Protecció del correu electrònic *62*
10.20 PROTECCIÓ DE LES INSTAL·LACIONS 62
10.21 GESTIÓ D'EXCEPCIONS 63
10.22 GESTIÓ D'IDENTITATS I AUTENTICACIÓ D'USUARIS 63
10.23 AUTORITZACIÓ DELS USUARIS ALS SISTEMES 63
10.24 DESENVOLUPAMENT SEGUR 65
10.25 ACCEPTACIÓ I POSTA EN SERVEI 65
10.26 PROTECCIÓ DE LES APLICACIONS I SERVEIS WEB 65
10.27 DADES DE PROVES 66
10.28 XIFRATGE 66
10.29 SIGNATURA ELECTRÒNICA 66
10.30 CERTIFICATS 67
10.31 PLA DE TRACES 67
10.32 INVENTARI D'ACTIUS 67
10.33 CONFIGURACIÓ DE SEGURETAT 67
10.34 MANTENIENT 68
10.35 ANTIMLWARE 68
10.36 CÒPIES DE SEGURETAT 69
10.37 EXPLOTACIÓ 69
10.37.1 Gestió de la configuració *69*
10.37.2 Gestió de canvis *69*
10.37.3 Protecció de claus criptogràfiques *70*
11 INFORMACIÓ ADDICIONAL I ACLARIMENTS **71**
12 ANNEX. I GESTIÓ DE SERVEIS TIC **72**
13 ANNEX II. PROTOCOL D'EMERGÈNCIES **72**

1 INTRODUCCIÓ

L'Ajuntament de Barcelona, amb el seu esperit de protegir la informació del ciutadà i els serveis que li ofereix, ha establert des de 2008 el servei de govern i administració d'identitats i accessos, un procés clau per al seu bon funcionament, ja que redueix els problemes d'accessos no autoritzats, així com la millora de la traçabilitat de les operacions i disminució dels costos d'administració.

En els últims anys, la transformació digital, el treball remot, l'automatització, els serveis que s'ofereixen en el Cloud i els accessos des de múltiples dispositius i tecnologies ens han portat a un escenari en el qual la identitat ha passat a ser el nou perímetre de seguretat que ha de facilitar reduir els riscos dels ciberincidents.

Actualment, l'Ajuntament de Barcelona té desplegat un sistema de gestió d'identitats basat en la tecnologia **Oracle Identity Manager** (d'ara endavant OIM), la qual, per la seva complexitat, volum d'informació gestionada i obsolescència de la versió instal·lada, presenta una sèrie de limitacions:

- Dificultat en la implementació de polítiques d'aprovisionament d'autoritzacions segons lloc de treball ocupat.
- Limitacions en la integració amb el repositori mestre d'identitats (SAP).
- Incidències en l'aprovisionament de comptes a/des dels sistemes.
- Problemes en l'eliminació de permisos davant la baixa dels usuaris i el seu cessament definitiu.
- Baix rendiment davant canvis en les polítiques.
- Implementació de mecanismes no estandarditzats (desenvolupaments propis).
- Incidències relacionades amb els canvis i sincronització de contrasenyes.
- Limitacions per a conèixer l'estat de les identitats i així poder tenir un control del que succeeix amb les identitats.
- Interfície poc amigable per als usuaris i administradors.

Ateses aquestes limitacions i l'evolució en els últims anys de la tecnologia de gestió i administració d'identitats, la solució actual no proporciona una resposta adequada ni flexible a les necessitats de l'Ajuntament de Barcelona. Per això, s'emprendrà un projecte de migració de la plataforma tecnològica que suporta els processos de gestió i administració d'Identitats i així, poder implantar els processos de govern d'identitats amb eficàcia i agilitat, tot donant resposta a les necessitades actuals i futures de l'Ajuntament de Barcelona.

Per tal que el nou sistema de Gestió d'Identitats pugui cobrir les necessitats de l'Ajuntament de Barcelona, es requereix la contractació d'un proveïdor especialitzat que disposi dels mitjans tecnològics i personal tècnic altament especialitzat per a complir amb els objectius.

En aquest document s'inclouen les especificacions d'aquesta licitació:

- Objecte i abast de la licitació.
- Descripció de la situació actual.
- Descripció i detall dels serveis a prestar.
- Requeriments de la nova solució.

- Informació que han d'aportar els licitadors.
- Criteri de valoració.
- Acords de nivell de servei.
- Clàusules i condicions generals.

2 ASPECTES GENERALS DEL CONTRACTE

2.1 OBJECTE

L'objecte del contracte és la implantació d'un nou sistema de govern i administració d'identitats i accessos per l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible.

2.2 ABAST I ÀMBIT DEL CONTRACTE

L'abast del contracte inclou les tasques següents:

- **Implantació d'un sistema de gestió i administració d'identitats i accessos, la migració de l'actual sistema, el llicenciament necessari del producte tecnològic i el corresponent suport per part del fabricant del producte.** La finalitat és la substitució de l'actual sistema de gestió d'identitats per un altre sistema que compleixi amb els requisits establerts i amb les mateixes funcions i processos implementats en el sistema actual (incloses aquells que han deixat de funcionar o no ho fan correctament).
    - Subministrament de llicències (compra) del producte ofert per a 26.000 identitats i per als connectors que siguin necessaris desplegar per a la migració. El llicenciament haurà de cobrir el desplegament de la tecnologia en dos entorns (productiu i no productiu) amb el mateix nombre d'identitats i els mateixos connectors. Seran vàlides per un període de 34 mesos (des de la fase d'instal·lació del producte fins a la finalització del contracte). En el cas de llicències per a la integració amb SAP, són necessàries l'aprovisionament de 16.000 identitats (personal intern).
    - Suport 24x7 per part del fabricant de la tecnologia davant incidències o fallades del producte i disponibilitat d'actualitzacions i pegats. Aquest suport tindrà una durada de 34 mesos (des del desplegament de la solució tecnològica fins a la finalització del contracte).
    - Implementació d'aquelles millores que s'identifiquin durant el procés de migració i durant tota la fase de prestació del servei.
- **Gestió de la nova plataforma d'identitats i accessos, que inclou:**
    - Serveis de vigilància de processos, recertificacions, qualitat de la dada, monitorització d'identitats i accessos, impuls de la millora contínua i evolutius sobre la plataforma de gestió d'identitats, etc.
    - Operació i administració de la nova plataforma de gestió d'identitats: actualitzacions, resolució d'incidències, implementació de millores i evolutius, nous connectors etc.

- Suport 24x7 per part del personal que opera la solució de gestió d'identitats per a la resolució de qualsevol tipus d'incident que es produeixi amb el sistema de gestió d'identitats o per al suport davant incidents greus de ciberseguretat que afectin l'Ajuntament de Barcelona. Aquest suport tindrà una durada de 34 mesos (des del desplegament de la solució tecnològica fins a la finalització del contracte).

  - Desenvolupament i desplegament d'evolutius sobre la plataforma actual (OIM) fins a la seva substitució per la nova plataforma.

- **Govern de la nova plataforma d'identitats de l'Ajuntament de Barcelona**.

L'àmbit d'aplicació funcional del sistema de Gestió d'Identitats de l'Ajuntament de Barcelona està constituït per unes 900 entrades d'organigrama en els següents ens. Tots ells, en major o menor mesura, formen part del sistema de Gestió d'Identitats[1].

- Gerències centrals
- Gerències de districtes
- Instituts públics
- Entitats de règim privat
- Consorcis
- Fundacions

Cal tenir en compte que, durant l'execució del projecte, és possible que es produeixin modificacions en l'estructura organitzativa.

En l'abast del sistema de gestió i administració d'identitats i accessos s'inclouen a tots els usuaris (empleats interns i externs) que accedeixen als recursos de l'Ajuntament de Barcelona i els seus Instituts Municipals. S'estimen aproximadament 26.000 identitats (16.000 identitats municipals i 10.000 externs i d'altres tipologies) distribuïdes en més de 500 centres.

3 SITUACIÓ ACTUAL

L'Ajuntament de Barcelona disposa d'un sistema de Gestió d'Identitats basat en Oracle Identity Manager (OIM) v11, amb el qual es gestionen unes 26.000 identitats aproximadament.

Entre les funcionalitats que permet actualment aquest sistema, destaquen les següents:

- Repositori d'identitats.
- Cicle de vida de les identitats.
- Aprovisionament de comptes a/des de sistemes.
- Contrasenya unificada per als sistemes.
- Autoservei de contrasenyes.
- Servei de suport a la gestió d'identitats externes i auxiliars (usuaris de servei, usuaris genèrics...).

[1] Organigrama disponible a L'organització | Ajuntament de Barcelona

3.1 ARQUITECTURA

Actualment, l'Ajuntament de Barcelona té desplegats els següents components de Oracle Identity Manager, tot executant-se sobre el sistema operatiu SUSE Linux Enterprise Server.

Component
JDK
Weblogic Server
Oracle IAM Suite
Oracle SOA Suite
Oracle Business Intelligence

Taula 1. Components de Oracle Identity Manager instal·lats

Al següent esquema es mostra l'arquitectura de servidors desplegada actualment de Oracle Identity Manager (OIM).

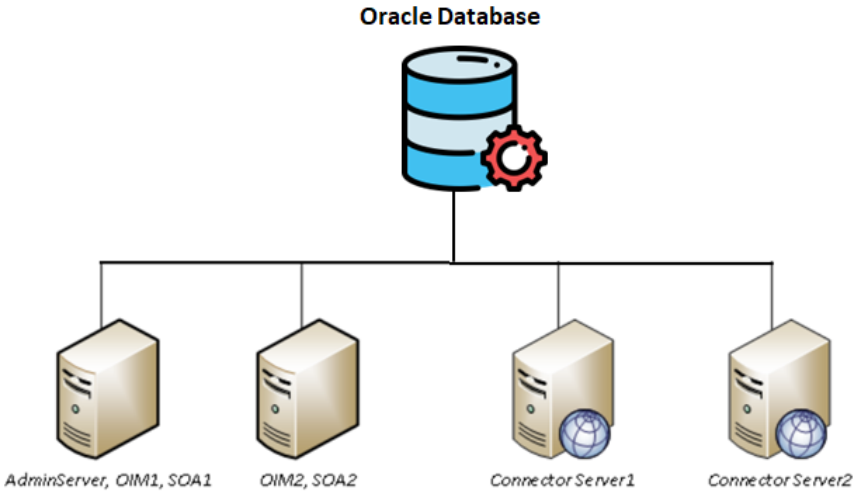


Ilustración 1. Arquitectura de servidores desplegada de OIM

3.2 SISTEMES INTEGRATS

El sistema actual de gestió d'identitats es sustenta de les següents dos fonts autoritzatives d'identitats (mestres):

Sistema	Descripció
SAP HR	Sistema des del qual s'aprovisionen els empleats de l'Ajuntament i l'organigrama corporatiu al sistema de gestió d'identitats. Des del sistema de gestió d'identitats també s'aprovisionen dades personals a SAP HR (adreça de correu, telèfon, etc.)
SAP de Parcs i Jardins	Directori des d'on s'aprovisionen els empleats de Parcs i Jardins.

Taula 2. Sistemes mestres d'aprovisionament d'identitats

A la següent taula es descriuen els sistemes que es troben integrats actualment amb Oracle Identity Manager mitjançant connectors on-line sincronitzats o processos diaris batch:

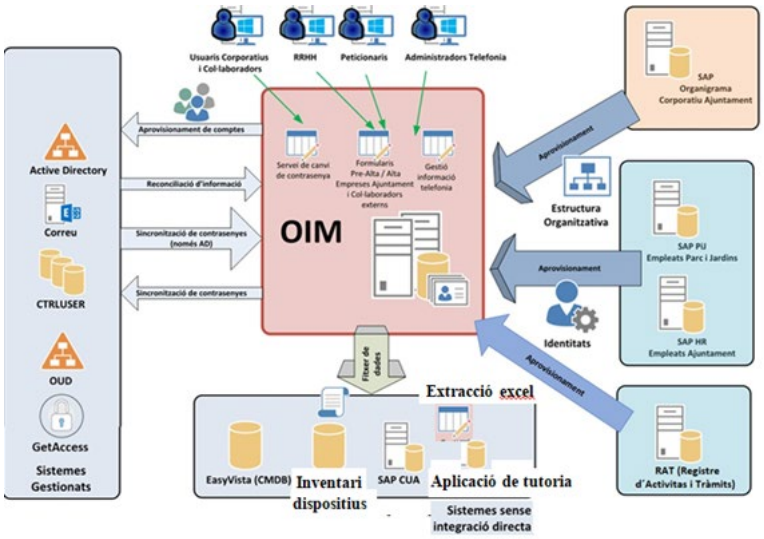
Sistema gestionat	Descripció
Active Directory	Directori contra el qual es validen les credencials d'accés a l'estació de treball, VPN, s'assignen les estacions virtuals, s'autoritza l'accés a unes certes aplicacions, etc.
Exchange	Directori de correu que emmagatzema les bústies corporatives de l'Ajuntament, tant els de domini bcn.cat com ext.bcn.cat.
Control User	Repositori central d'autoritzacions d'accés a aplicacions de l'Ajuntament, tant per aplicacions modernes com per aplicacions *"legacy"*. Connector de tipus LDAP.
OUD (Oracle Unified Directory)	Repositori central que gestiona les autoritzacions d'accés a les aplicacions modernes i l'autenticació/autorització del proveïdor d'identitats corporatiu, així com les credencials de segon factor dels usuaris. Connector de tipus LDAP.
SAP CUA	SAP Central User Administration. Directori on es gestionen els usuaris dels sistemes SAP.
EasyVista	Sistema CMDB. Actualment se sincronitza el compte dels usuaris mitjançant la generació d'un fitxer de text, però no la seva contrasenya.
GetAccess	Eina per a l'autenticació d'usuaris utilitzada per alguns sistemes. Connector de tipus API Rest.
RAT	Sistema RAT (Registre d'Activitats i Tràmits). Sistema que proporciona informació addicional de les identitats.

Taula 3. Sistemes als que s'aprovisionen comptes directament

També existeixen formularis per a donar d'alta noves identitats i mantenir actualitzada la seva informació. A continuació, s'enumeren algun d'ells:

- Formulari per a la gestió de la informació de telefonia.
- Formulari de pre-alta de usuaris.
- Formulari per a la gestió d'empreses de l'Ajuntament.
- Formulari per a la gestió de col·laboradors externs.
- Formulari per al canvi de contrasenya.
- Etc.

En el següent esquema es mostren els sistemes integrats actualment amb OIM.



Il·lustració 2. Esquema amb els sistemes integrats amb OIM

3.2.1 Núvol de Microsoft

Les identitats corporatives també se sincronitzen a Microsoft Entra ID, per a l'ús del correu corporatiu al núvol, l'adopció d'Office 365 i, en general, per a l'ús de totes aquelles eines i funcionalitats *cloud* que Microsoft ofereix (o pugui oferir en un futur) i que siguin d'interès per l'Ajuntament de Barcelona i/o l'IMI.

3.3 TIPOLOGIA D'IDENTITATS

A l'Ajuntament de Barcelona es gestionen els següents tipus d'identitats:

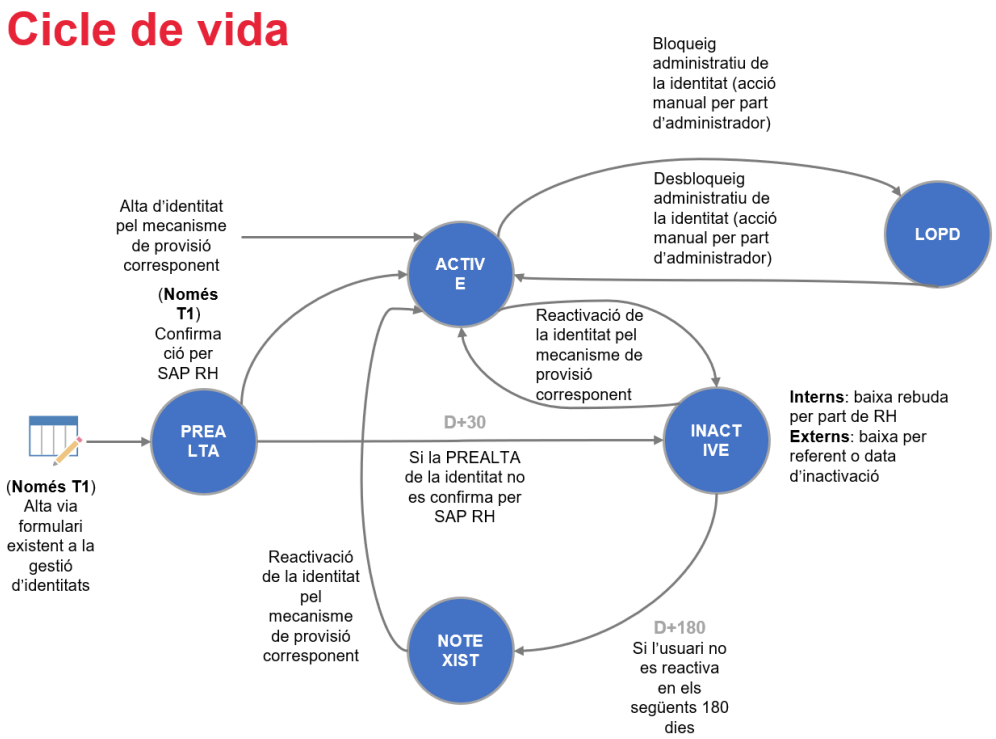
- **T1:** Personal intern de l'Ajuntament les dades personals del qual i professionals són gestionats des de l'eina SAP de Recursos Humans.
- **T3:** Personal intern de l'Ajuntament, concretament d'empreses públiques associades a l'Ajuntament (BSM, Barcelona Activa, etc.), però la gestió de la qual no està centralitzada en l'eina SAP de Recursos Humans.
- **T4:** Personal extern que col·labora d'alguna forma amb l'Ajuntament i necessita accés als principals sistemes d'informació de l'Ajuntament.
- **T11:** Personal intern de l'Ajuntament associat al col·lectiu de Parcs i Jardins, les dades personals dels quals i professionals són gestionats des d'un SAP propi de Parcs i Jardins.
- **G1:** Comptes genèrics, principalment per a representar identitats que poden utilitzar més d'un usuari físic.
- **S1:** Comptes de servei, utilitzades per aplicacions, connectors, etc.

3.4 CICLE DE VIDA DE LES IDENTITATS

Les identitats tenen assignat un dels següents estats:

- **PREALTA:** estat en el qual es troba una identitat de tipus T1 quan es dona d'alta manualment mitjançant els formularis desenvolupats a aquest efecte en el sistema de Gestió d'Identitats, previ a la seva alta en SAP HR. Té com a finalitat que l'usuari tingui accés als sistemes d'informació de l'Ajuntament fins que sigui donat d'alta en l'eina SAP de Recursos Humans.
- **ACTIVE:** estat en el qual es troba la identitat mentre està treballant per a l'Ajuntament i permet l'accés als diferents sistemes d'informació de l'Ajuntament.
- **INACTIVE:** estat de la identitat quan deixa d'ocupar un lloc de treball a l'Ajuntament (personal intern) o arriba la data de finalització de la seva relació professional amb l'Ajuntament (col·laboradors externs de tipus T4) o bé, el seu gestor De Recursos Humans. no renova la seva vinculació (per a empreses públiques amb usuaris de tipus T3 no provinents de SAP). A les identitats que es troben en aquest estat, les hi desactiva l'accés a tots els sistemes d'informació de l'Ajuntament, encara que no se li eliminen els drets d'accés atorgats al llarg de la seva vida a l'Ajuntament.
- **NOTEXIST:** estat al qual passa la identitat quan porta més de 6 mesos en estat INACTIVE. Es treuen tots els permisos, però es manté la identitat.
- **LOPD:** estat de la identitat quan es volen desactivar els accessos de manera manual quan sigui necessari per temes de seguretat, tot indicant l'estat directament en el sistema de gestió d'identitats.

En el següent esquema es mostra el cicle de vida de les identitats a l'Ajuntament de Barcelona.



Il·lustració 3. Cicle de vida de les identitats

Els **canvis de tipologia d'identitat més rellevants** són els següents

- Pas d'intern (T1/T11) a col·laborador extern (T4).
- Pas de col·laborador extern (T4) a intern (T1/T11).

Existeixen diferents processos de **canvis organitzatius** dins de l'Ajuntament:

- **Moviments d'identitats entre organitzacions:** es tracta de moviments d'identitats d'una organització origen a una organització destinació
- **Canvis en dades de les organitzacions:** es modifiquen atributs de l'organització a partir de les dades provinents de SAP
- **Moviments d'organitzacions**: procés pel qual una organització passa a dependre d'una altra jeràrquicament.
- **Baixes d'usuaris:** quan els usuaris passen a estats INACTIVE i NOTEXIST.

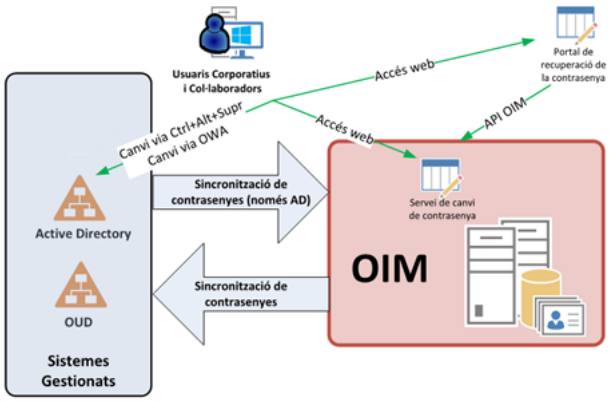
Cal remarcar la importància d'aquests canvis i la seva sincronització als sistemes gestionats (Active Directory i Exchange entre altres), ja que moviments de branques en Active Directory poden provocar canvis en l'aplicació de polítiques, i canvis en la informació dels atributs, la qual cosa comporta canvis de permisos en el correu o llistes de distribució.

També està implementat un procediment per a la **gestió del cicle de vida de comptes genèrics o de servei** així com els usuaris privilegiats. Quan es necessita un nou compte genèric o de servei, es realitza una sol·licitud d'alta i, després de la seva aprovació, es procedeix a la seva alta i assignació de credencials. Existeix un procediment de revisió d'aquesta mena de comptes mitjançant el qual, transcorregut un any des de la seva alta, es notifica al seu responsable la pròxima caducitat del compte genèric o de servei perquè procedeixi a la seva renovació.

Els usuaris privilegiats d' eines i servidors, en la mesura que sigui possible s'autenticaran a l'AD i restaran en un Grup (GPO), i tindran un usuari adm_codiusuari.

3.5 SINCRONITZACIÓ DE LA CONTRASENYA

En el següent diagrama es mostren els diferents sistemes amb els quals es realitza una sincronització de la contrasenya:



Il·lustració 4. Procés de sincronització de contrasenyes

- **Active Directory:** contrasenya per a accedir a l'estació de treball corporativa, a l'estació virtual, correu corporatiu, VPN, etc.
- **OUD:** contrasenya per a accedir a totes les aplicacions protegides pel proveïdor d'identitats corporatiu (OAM).

4 DESCRIPCIÓ DE LES TASQUES OBJECTE DEL CONTRACTE

4.1 GOVERNANÇA DE LES IDENTITATS

Les prestacions objecte del contracte han de facilitar eines de Govern Municipal per a minimitzar els riscos de seguretat de la informació i donar compliment a la normativa vigent del reglament de l'Esquema Nacional de Seguretat (ENS) i de Protecció de Dades i Privacitat.

El Govern de les Identitats i els Accessos fa referència al conjunt de polítiques i processos que fan que qualsevol identitat tingui atorgades les autoritzacions, dispositius i recursos necessaris per a desenvolupar les seves tasques seguint el principi bàsic de l'ENS de mínim privilegi i de mínim temps possible.

Per a garantir aquest propòsit la Governança de les identitats es prestaran d'acord a les directrius municipals i de forma específica les establertes per la Direcció de Serveis de Seguretat de la Informació. Aquesta direcció defineix el model i la gestió de la seguretat de les identitats, accessos, credencials i autoritzacions, així com els indicadors, les polítiques i les normes que les regulen, assegurant el seu encaix en els programes de ciberseguretat de l'Ajuntament liderats per la mateixa Direcció.

La governança d'identitats ha de vetllar per la seguretat dels sistemes d'identificació de l'Ajuntament, cooperar en la definició i transformació dels seus models de seguretat. Així mateix, ha d'avaluar els riscos i proposar mesures tècniques i organitzatives òptimes i proporcionals per mitigar-los. Per assolir aquest objectiu, el govern de les identitats es desenvoluparà de manera coordinada amb la Direcció de Serveis de Seguretat de la Informació, assegurant un enfocament integrat i alineat amb els programes de ciberseguretat municipals.

La prestació de les funcions associades a la governança d'identitats durant la durada inicial del contracte (36 mesos) es realitzarà en dues fases:

- Estabilització del servei de governança de les identitats durant els primers 34 mesos i de forma paral·lela a la implantació de la nova eina de gestió d'identitats.
- Manteniment del servei de governança (servei operatiu al 100%) els darrers 2 mesos de la durada inicial del contracte.

Els objectius dels serveis de governança de les identitats i accessos són:

- Formalitzar el model de supervisió de la seguretat de les identitats i accessos de l'Ajuntament de Barcelona
- Consolidar la funció d'arquitecte de seguretat en el procés de transformació i evolució de solucions corporatives de gestió d'identitats i accessos, entenent com a arquitecte d'identitats la visió holística de processos, models d'integració, cicles de vida, credencials, controls d'accés, models d'autoritzacions, etc. En definitiva el govern de qui fa que en la organització amb el principi del mínim privilegi

- Impulsar el desplegament d'iniciatives Zero Trust centrades en l'àmbit de la identitat digital.

L'adjudicatari haurà de realitzar les següents activitats:

- Definir tasques i fer el seguiment del compliment d'objectius establerts per seguretat en la gestió de riscos de seguretat de les identitats.
- Revisar i alinear l'estratègia d'implantació del sistema de gestió d'identitats i control d'accessos amb les necessitats de l'Ajuntament de Barcelona.
- Analitzar problemes i indicar millores relacionats amb el govern d'identitats i proposar solucions.
- Proposar actuacions per resoldre riscos de seguretat relacionats amb la seguretat en el control d'accessos i model d'autoritzacions.
- Proposar actuacions derivades de millores i reducció de riscos del sistema de credencials d'accés.
- Definir i impulsar el desplegament d'iniciatives Zerotrust centrades en l'àmbit de la identitat digital, coordinant-se amb la resta d'actors implicats de l'IMI.
- Proposar actuacions per la implementació del model de governança de les identitats per tal de complir amb els requeriments de seguretat i les necessitats de negoci de l'Ajuntament de Barcelona
- Participar amb projectes i iniciatives per a la construcció i evolució del model de seguretat de noves tecnologies en relació a la identitat.
- Participar com a arquitecte de seguretat en el procés de transformació i evolució de solucions corporatives de gestió d'identitats, gestió de comptes privilegiades, autenticació i SSO, autorització i control d'accés a recursos, gestió de claus avaluant i proposant els requeriments de seguretat escaients i fent seguiment de la seva correcta implantació.
- Analitzar els requeriments i proposar solucions per a la integració de nous sistemes amb la plataforma de gestió d'identitats.
- Proposar requeriments en base a les directrius de seguretat i donar suport a la implantació de sistemes de control d'accessos i principi de mínim privilegi.
- Analitzar, proposar millores i adaptar el cicle de vida de les identitats per a la seva adequació a les noves necessitats.
- Proposar directrius i donar suport a la implantació d'una gestió de comptes privilegiats.
- Anàlisi d'informes relacionats amb la gestió d'identitats per tal de detectar problemes i proposar millores.
- Proporcionar formació i assessoria sobre gestió d'identitats i accessos.
- Assistència a les reunions en les quals sigui necessari tractar algun tema relacionat amb la gestió d'identitats i accessos.

- Mantenir-se permanentment actualitzat sobre el marc legal, normatiu, bones pràctiques i tendències del mercat en relació a la gestió d'identitats, signatura electrònica i la criptografia.
- Previ a la finalització del contracte, haurà de contemplar-se un termini de transició del servei. Com a part d'aquesta transició del servei s'espera, almenys, la següent documentació:
    - Estat actual de la identitat
    - Full de ruta de les tasques en curs
    - Proposta de tasques a realitzar
- Recopilar i conèixer els mecanismes d'identificació, autenticació, control d'accés i dels diferents sistemes d'informació de l'Ajuntament de Barcelona gestionar i fer el seguiment dels riscos identificats per seguretat que se'n derivin.
- Donar suport explícit i directe a la Direcció de Seguretat de la Informació en els serveis de Compliment Normatiu, Gestió de Riscos, auditories i Ajbcn-SOC per a la gestió segura de la identitat digital i els accessos segurs.
- Suport a les auditories i revisions de qualitat, en la revisió i elaborar propostes de millora de tots els processos i procediments (funcionals i tècnics) d'identitats control de la integritat i consistència de les dades entre els diferents sistemes (revisió permanent de les sincronitzacions i integracions), vigilància de comptes orfes etc.
- Planificar les tasques per tal d'alimentar el quadre de comandament de seguretat orientat a la gestió d'identitats i accessos de riscos de seguretat de les identitats, que ens permeti fer el seguiment dels
- Elaborar reports periòdics o puntuals sobre sistema d'informes de les identitats i accessos segons el què estableixi la direcció de Seguretat(sota la premissa del coneixement permanent de "qui fa què i quan"), pel coneixement i control de la seguretat de la informació, de manera que les direccions i gerències de Ajuntament tinguin visibilitat i control sobre el personal i els sistemes d'Informació dels que en són responsables. L'adjudicatari elaborarà i lliurarà, com a mínim, els següents informes de lliurament recurrent:
    - Informes sota demanda o recurrents de compliment de sistemes d'informació a Gerències de Ajuntament
    - Informe mensual de compliment de la política de contrasenyes i d'altres credencials
    - Informe mensual d'indicadors d'identitats i accessos.
    - Informe mensual d'indicadors accessos remots
    - Informe específic que se sol·liciti arrel d'alguna actuació que requereixi d'indicadors puntuals.
- Generar i implantar informes per a les recertificacions del personal

- Recopilar i conèixer els mecanismes d'identificació, autenticació, control d'accés i dels diferents sistemes d'informació de l'Ajuntament de Barcelona coordinar el seguiment de riscos de seguretat que se'n deriven.
- Creació d'un model de maduresa per a la gestió de la identitat: Desenvolupar un model de maduresa específic per avaluar el grau d'implementació i efectivitat del sistema de gestió d'identitats i accessos, incloent recomanacions per a la seva millora contínua.
- Gestió de la identitat federada: Proposar i implementar mecanismes de federació d'identitats que permetin integrar-se de forma segura amb terceres parts, assegurant el control dels accessos i l'autenticació en entorns híbrids o col·laboratius.
- Plans d'impacte i continuïtat del servei: Desenvolupar i mantenir plans específics d'impacte i recuperació per assegurar la continuïtat del sistema de gestió d'identitats davant incidents de seguretat o fallades tècniques.
- Programa de ciberresiliència per a la identitat: Desenvolupar un programa que defineixi mesures de protecció, detecció, resposta i recuperació en casos de ciberatacs dirigits a la gestió d'identitats.
- Adaptació als entorns multi-cloud: Garantir que el sistema de gestió d'identitats s'integra correctament amb entorns multi-cloud, assegurant coherència en l'autenticació i el control d'accessos a recursos distribuïts.
- Anàlisi d'impacte de l'usuari final: Realitzar estudis periòdics per assegurar que els processos de gestió d'identitats són intuïtius i compatibles amb les necessitats de l'usuari final, minimitzant friccions.
- Indicadors d'eficiència operativa: Implementar mètriques específiques per mesurar no només la seguretat, sinó també l'eficiència operativa del sistema, com el temps mitjà per resoldre problemes d'accés o la velocitat d'implementació de nous processos.

4.2 GESTIÓ I CONTROL D'IDENTITATS, ACCESSOS, AUTENTICACIONS I AUTORITZACIONS

L'Adjudicatari proveirà un servei de gestió de les identitats i accessos amb una visió integral, que va més enllà d'allò estrictament tècnic i operatiu. Aquest servei es prestarà d'acord a les indicacions i requeriments definits per l'IMI, tenint especialment en compte les directrius de la Direcció de Serveis de Seguretat de la Informació.

L'Institut Municipal d'Informàtica podrà sol·licitar que es proveeixin els serveis descrits en aquest apartat també en relació als processos i procediments implantats sobre l'actual sistema de gestió d'identitat (basat en OIM), des de l'inici de la vigència del contracte fins l'aturada de la plataforma actual de gestió d'identitats.

La realització de les activitats mínimes descrites en aquest subapartat 4.2 associades a la gestió i control d'identitats, accessos, autenticacions i autoritzacions durant la durada inicial del contracte (36 mesos) es realitzarà en dues fases:

- Estabilització dels serveis de gestió i control d'identitats, accessos, autenticacions i autoritzacions durant els primers 34 mesos i de forma paral·lela a la implantació de la nova eina de gestió d'identitats.
- Manteniment dels serveis de gestió i control d'identitats, accessos, autenticacions i autoritzacions (servei operatiu al 100%) els darrers 2 mesos de la durada inicial del contracte.

Descripció de les activitats mínimes:

- Revisió i execució de processos definits per l'IMI relatius a la integritat i consistència de les dades entre els diferents sistemes, revisió recurrent de les sincronitzacions i integracions i connectors, vigilància de comptes orfes etc.

- Processos de recertificacions i de millora de la qualitat de repositoris, segons les polítiques i recomanacions establertes per l'IMI.

- Suport evolutiu i preventiu de la gestió d'identitat, cobrint com a mínim:
    - Revisió de que els processos de l'eina funcionen correctament.
    - Revisió periòdica de tasques d'aprovisionament a sistemes d'informació fallides
    - Revisió periòdica de tasques de reconciliació des de sistemes d'informació fallides
    - Suport incidental de la plataforma (sincronització de contrasenya, sincronització d'informació amb sistemes d'informació integrats, accés a la plataforma, problemes amb gestió de peticions / recertificacions, etc.)
    - Consultes sobre la plataforma (dubtes sobre cicle de vida, sistemes integrats, funcionament dels fluxos de petició / recertificació, informes, etc.)
    - Treballar amb el fabricant de la solució per tal de corregir problemes o incidències sobre la plataforma

- Implementació d'evolutius relacionats amb la gestió d'identitats que puguin sorgir durant la vigència del contracte, alguns exemples d'evolutius en base a l'anterior contracte de govern d'identitats són:
    - Modificació de la integració amb les fonts autoritzatives d'identitats (SAP RH, SAP PiJ, etc.)
    - Creació/modificació de formularis per la gestió d'usuaris externs, genèrics o de servei
    - Connectors amb sistemes no integrables, via enviament/recepció de fitxers i representació de dades a la GID
    - Implementació de connectors directes amb nous sistemes d'informació, tal i com SAP's, aplicacions al núvol, MS Teams, AWS, etc.
    - Execució de projectes i iniciatives de perfilat de sistemes per tal d'automatitzar el perfil i l'assignació de recursos dels usuaris a cadascun dels sistemes finals
    - Desenvolupaments de portals específics per millorar els processos d'identitat (gestió d'usuaris externs, portals de gestió de la contrasenya, etc.)
    - Implementació de nous fluxos d'aprovació/recertificació (per demanar certs permisos, recertificar permisos o usuaris, etc.)
    - Desenvolupaments per la generació de nous indicadors/informes

- Gestió i manteniment del cicle de vida de l'usuari: implantació i vigilància de tots els fluxos relacionats amb el cicle de vida dels usuaris i de totes les accions i processos que

es deriven de les altes, baixes, canvis d'estat, canvis de departament, canvis en les dades de l'usuari, jubilacions, baixes de llarga durada, canvis de responsable etc.

- Implantació o vigilància de la provisió automàtica de recursos i autoritzacions i sincronismes bidireccionals, avançant en la direcció de l'establiment d'un perfilat en base a categories de lloc de treball i posicions, per simplificar, agilitzar, homogeneïtzar i centralitzar les assignacions de recursos.

- Gestió de les credencials. Implantació i vigilància del compliment de la política de contrasenya corporativa; executar iniciatives de canvis globals o massius de credencials o polítiques.

- Implementació de polítiques de seguretat, processos i revisió i monitoratge d'usuaris genèrics i usuaris de servei.

- Control dels accessos privilegiats. Revisió permanent sota la premissa de mínim privilegi i mínim temps possible en base a les directrius de seguretat establertes pel grup de Governança d'identitats.

- Implementació de polítiques i monitoratge d'autenticacions i autoritzacions.

- 2FA. implementació i supervisió de les polítiques de seguretat establertes i monitoratge dels accessos i serveis 2FA.

- Integració amb un nou 2FA, actualització d'algun existent.

- Implantació de canvis tant en el model d'identitats (cicle de vida de l'usuari, integracions, processos...) com en la plataforma de gestió d'identitats, d'acord a nous requeriments de seguretat, a millores indicades per l'IMI o identificades pel grup de Governança d'Identitats, a l'evolució dels diferents sistemes integrats i, en general, a les necessitats dels processos de negoci de l'Ajuntament de Barcelona. Per exemple, introducció de nous tipus d'usuaris, implementació de nous estats dels usuaris -per exemple, un nou estat per al personal que ja no treballa a l'Ajuntament de Barcelona, però continua necessitant accedir a alguns sistemes-, modificació de les dades de la identitat (inclusió, supressió o modificació de camps), adequació a canvis organitzatius i d'organigrama (especialment, arrel del canvi de mandat), noves integracions i sincronitzacions, automatització de processos etc.

- Tasques i activitats de suport necessàries per a garantir una correcta planificació i execució dels projectes de l'IMI relacionades amb les identitats, des del vessant de l'operació i gestió d'identitats i accessos (per exemple identificant potencials implementacions/evolutius) amb el propòsit d'aconseguir l'objectiu final amb el temps establert i amb el nivell de qualitat exigit.

- Atenció i resolució de dubtes i suport tècnic i operatiu especialitzat en matèria de Seguretat de les identitats i accessos per a les diferents àrees i departaments de l'Ajuntament i l'IMI.

4.3 IMPLANTACIÓ D'UNA NOVA EINA DE GESTIÓ I ADMINISTRACIÓ D'IDENTITATS I ACCESSOS

A part de complir tot allò establert en aquest apartat 4.3, la nova eina també haurà de complir tots els requeriments descrits al punt 6.

La implantació del nou sistema de gestió d'identitats no ha de tenir impacte en l'operativa diària de l'Ajuntament de Barcelona ni en els seus usuaris, havent de conviure tots dos sistemes fins a la parada definitiva de l'actual sistema. Com a part del procés de migració, s'haurà de minimitzar l'impacte en la contrasenya actual dels usuaris perquè pugui continuar realitzant les seves funcions de manera transparent.

El projecte de posada en marxa de la nova eina s'estructurarà en 5 fases:

4.3.1 Fase I - Anàlisi inicial del projecte

En aquesta fase, l'adjudicatari realitzarà una anàlisi de la situació actual de les eines de gestió de la identitat de l'Ajuntament de Barcelona i dels processos implementats, tot desenvolupant per a això totes les activitats necessàries que permetin a l'adjudicatari obtenir el coneixement necessari per a l'elaboració del pla de treball.

La durada prevista d'aquesta fase és d'**un mes** i s'han de realitzar, com a mínim, les següents activitats:

- S'establirà un pla de treball per a tota aquesta primera fase:
    - Identificació d'interlocutors.
    - Planificació de les entrevistes amb tots els responsables d'àrea que s'identifiquin i que siguin clau per a la consecució del projecte.
- Es disposaran qüestionaris i sol·licituds d'informació per a concretar el màxim possible les entrevistes.
- S'analitzarà la infraestructura tecnològica que dona suport a l'actual solució de gestió d'identitats.
- S'analitzaran els processos implementats actualment.

S'esperen, com a mínim, els següents lliurables:

- Abast del projecte.
- Anàlisi de la situació actual.

4.3.2 Fase II – Disseny de la solució del projecte

En aquesta fase s'analitzarà tota la informació recopilada en la fase anterior i es dissenyarà la solució de gestió d'identitats a implementar a l'Ajuntament de Barcelona. El disseny de la solució ha de complir amb els requeriments establerts en el capítol 6 *"Requeriments de la nova solució de gestió d'identitats"*.

Aquest disseny contemplarà la migració de tots els processos de l'anterior sistema al nou, així com la implementació d'aquelles millores identificades i consensuades amb l'Ajuntament de Barcelona. La durada prevista d'aquesta fase és d'**un mes** i es faran les següents tasques:

- Definició detallada del model de gestió d'identitats per a implantar a l'Ajuntament de Barcelona.
- Revisió i millora de les tipologies d'identitats.
- Revisió i millora de l'organigrama de negoci.
- Revisió i millora del cicle de vida de la identitat.
- Disseny d'arquitectura d'alt i baix nivell.
- Definició dels casos d'ús.
- Definició dels processos de certificació.
- Definició de la traçabilitat i l'acompliment.
- Disseny del pla de desplegament i estratègia de migració.
- Disseny del futur trasllat de la plataforma a un cloud gestionat per l'IMI.
- Pla de proves.
- Definició dels processos de monitorització proactiva tant de la plataforma tecnològica com dels processos vinculats al cicle de vida de la identitat i les integracions amb altres sistemes
- Definició del catàleg de peticions de servei i la matriu d'escalat d'incidències pel nou servei.
- Definició dels processos de backup de les dades i la plataforma. Elaboració també d'un Disaster Recovery Plan (DRP).
- Plans de formació, comunicació i divulgació als agents involucrats.

S'esperen, com a mínim, els següents lliurables:

- Disseny de la solució per a desplegar.
- Arquitectura del sistema.
- Casos d'ús.
- Pla de desplegament i migració.
- Anàlisi d'impacte.
- Pla de proves.
- Pla de comunicació.

4.3.3 Fase III – Desplegament del projecte del nou gestor d'identitats

En aquesta fase es realitzarà el desplegament de la tecnologia (software) de gestió d'identitats d'acord amb el disseny establert i consensuat amb l'Ajuntament de Barcelona.

La infraestructura base on s'instal·larà el sistema de gestió d'identitats serà proporcionada per l'Ajuntament de Barcelona (maquinari/sistema de virtualització, sistema operatiu i base de dades amb les llicències necessàries).

La durada prevista d'aquesta fase és d'**un mes** i s'hauran de dur a terme les següents activitats, no excloent qualsevol altra activitat que sigui crítica per a la consecució de la fita:

- Desplegament de la tecnologia de gestió d'identitats en dos entorns, *"productiu"* i *"no productiu"*, en les instal·lacions de l'Ajuntament de Barcelona.
- Proves unitàries.
- Proves de rendiment.
- Proves d'acceptació.
- Posada en marxa dels processos de monitorització definits durant la fase II
- Proves de backup, restauració de backup i simulacre de Disaster Recovery Plan (DRP).
- Acceptació de servei i transició del servei (pas a producció): posada en marxa de les noves peticions de servei i activació de la matriu d'escalat d'incidències del nou servei, integració amb els serveis d'observabilitat de l'IMI... . Es treballarà conjuntament amb els equips de l'IMI corresponents a tal efecte (Acceptació de servei, SMO, Oficina Tècnica d'Explotació, SAU, equips tècnics vinculats amb l'operació de l'eina -com ara CPD, OSAT..., equips tècnics del serveis integrats amb la nova eina de gestió d'identitats...)
- Lliurament de llicències.

S'esperen, com a mínim, els següents lliurables:

- Descripció tècnica del desplegament realitzat.
- Informe dels treballs realitzats.

Al final d'aquesta fase III, l'adjudicatari començarà a administrar la a nova eina desplegada segons els requeriments definits al punt 4.4.

4.3.4 Fase IV – Redefinició i migració de l'actual sistema de gestió d'identitats

En aquesta fase es realitzarà una migració de tots els processos que estan implantats actualment en el sistema de gestió d'identitats al nou sistema, incloent-hi aquelles millores poguessin identificar-se.

Durant el procés de migració hauran de conviure tots dos sistemes de gestió d'identitats sense impacte en els usuaris ni en l'operativa de l'Ajuntament.

És responsabilitat del licitador l'Identificar els usuaris, organismes, processos i activitats que es veuran afectades en termes de disponibilitat, així com identificar l'impacte dels canvis realitzats.

La durada prevista d'aquesta fase és de **18 mesos** i s'hauran de dur a terme les següents activitats:

- Migració de totes les identitats i processos existents actualment als entorns *"productiu"* i *"no productiu"*, inclosos aquells processos que actualment poguessin presentar fallades i que hauran de solucionar-se en la nova implantació:
    - Configuració del model de dades.
    - Càrrega de dades.
    - Implementació del cicle de vida de les identitats.

  - Implementació del cicle de vida de comptes genèrics i comptes de servei.
  - Migració dels connectors existents actualment: SAP HR, SAP de Parcs i Jardins, SAP CUA, Active Directory, Exchange, Control User, OUD.
  - Migració de tots els formularis existents actualment per a la gestió d'identitats.
  - Migració de scripts.
  - Migració de treballs (*"Jobs"*).
  - Migració de polítiques.
- Migració de l'estructura organitzativa.
- Migració del model de rols i permisos existent actualment.
- Proves unitàries.
- Proves d'acceptació.
- Posada en marxa dels processos de monitorització definits durant la fase II
- Proves de backup, restauració de backup i simulacre de Disaster Recovery Plan (DRP).
- Acceptació de servei i transició del servei (pas a producció): posada en marxa de les noves peticions de servei i activació de la matriu d'escalat d'incidències del nou servei, integració amb els serveis d'observabilitat de l'IMI... . Es treballarà conjuntament amb els equips de l'IMI corresponents a tal efecte (Acceptació de servei, SMO, Oficina Tècnica d'Explotació, SAU, equips tècnics vinculats amb l'operació de l'eina -com ara CPD, OSAT..., equips tècnics del serveis integrats amb la nova eina de gestió d'identitats...)

S'esperen, com a mínim, els següents lliurables:

- Documentació amb la descripció dels processos implantats (model de dades, cicle de vida de les identitats, connectors, formularis, rols, permisos, etc.).
- Informe de treballs realitzats.
- Informe de seguiment del projecte.

4.3.5 Fase V – Aturada de la plataforma actual de gestió d'identitats

Un cop validada la nova solució de Gestió d'Identitats amb tots els seus processos implantats, es procedirà a aturar la plataforma actual de Gestió d'Identitats de l'Ajuntament de Barcelona.

Previ a realitzar aquesta aturada, s'haurà de verificar que la seva aturada no té cap impacte en l'operativa de l'Ajuntament de Barcelona.

4.4 ADMINISTRACIÓ, OPERACIÓ I EVOLUCIÓ DE LA NOVA EINA DE GESTIÓ D'IDENTITATS

Els serveis descrits en aquesta apartat començaran a proveir-se a partir del final de la fase III del projecte d'implantació de la nova eina (detallat en el punt 4.3).

La realització de les activitats descrites en aquest subapartat 4.4 associades a l'administració, operació i evolució de la nova eina de gestió d'identitats durant la durada inicial del contracte (36 mesos) es realitzarà en dues fases:

- Estabilització dels serveis d'administració, operació i evolució de la nova eina de gestió d'identitats des del final de la fase III del projecte d'implantació de la nova eina (detallat en el punt 4.3) fins el 34è mes des de l'inici del contracte.
- Manteniment dels serveis d'administració, operació i evolució de la nova eina de gestió d'identitats (servei operatiu al 100%) els darrers 2 mesos de la durada inicial del contracte.

L'adjudicatari proveirà els següents serveis:

- **Administració integral del nou sistema de gestió d'identitats:**
    - Monitoratge permanent del servei, garantint la disponibilitat de la plataforma.
    - Revisió periòdica i diària de la infraestructura i indicadors de servei, documentant diàriament:
        - Estat de l'eina
        - Revisió logs processos
        - Resolució de peticions
        - Resolució d'incidències
    - Realització de processos més puntuals:
        - Resolució de problemes.
        - Actuacions puntuals sobre la GID
        - Proposar millores
        - Proposar evolutius
    - Actuacions urgents en l'àmbit de la ciberseguretat:
        - Actualització urgent de components GID.
    - Configuració i gestió de software associat als components del servei.
    - Gestió de la configuració del sistema.
    - Suport als processos de gestió i explotació.
    - Administració de dades.
    - Manteniment dels connectors amb els sistemes integrats.
    - Integració de nous sistemes amb gestió d'identitats, o modificació dels existents. Per exemple, la integració amb Microsoft Entra ID i GetAccess, un cop conclosa la migració de OIM a la nova plataforma de gestió d'identitats.
    - Implementació de noves funcionalitats o canvis que se sol·licitin (gestió de rols, implementació de fluxos de treball, nous formularis, etc.)
    - Operacions massives sobre identitats, rols, aplicacions, etc.

- Revisió de problemes de seguretat que puguin afectar a la plataforma i serveis que composen la solució.
- Revisió usuaris orfes:
  - Usuaris externs amb referents que no estan actius (que s'han jubilat, canviat de departament, etc.)
  - Comptes que existeixen als sistemes finals i no a la GID
- Revisió de la qualitat de les dades dels usuaris:
  - Recertificació dels usuaris T3:
    - Recertificació dels referents de RRHH de cadascuna de les companyies
    - Recertificació dels usuaris per part dels referents de RRHH
  - Recertificació de referents de T4
    - Recertificació referents amb els seus usuaris, que ho continuen essent
    - Recertificació de referents inactius
    - Correus avís usuaris T4 sense activitat
  - Recertificació d'usuaris genèrics i de servei
    - Recertificació d'usuaris sense ús
    - Renovació periòdica de credencials
    - Renovació de la data d'inactivació
  - Revisió de que les dades als sistemes finals integrats estiguin alineades amb les de la GID
- Manteniment dels fluxos d'aprovació i Recertificació d'usuaris i permisos creats
- Llançament de campanyes periòdiques de Recertificació de permisos
- Implementació de polítiques de seguretat definides per l'equip de seguretat de l'IMI
  - Polítiques de contrasenyes corporatives
  - Càlcul de riscos dels usuaris en base a paràmetres
  - Desactivació d'usuaris per incident de seguretat
- Renovació contrasenyes
  - Emissió de llistes d'usuaris segons criteris
  - Aplicació de dades d'excels a GID
- Desenvolupament de nous tipus d'informes de governança d'identitats quan siguin necessaris.
- Resolució de peticions de servei.
- Realització de còpies de seguretat.
- Extracció de dades i elaboració dels informes requerits per l'Institut Municipal d'Informàtica i l'Ajuntament de Barcelona.

- **Monitoratge del sistema**
  - Monitoratge proactiu de l'estat dels components.
  - Definició contínua d'alertes.
  - Informes d'alertes, incidències i activitat.
- **Evolució de la plataforma:**
  - Aplicar els pegats requerits per temes de ciberseguretat en el menor temps possible.

- Actualització de versions i instal·lació de pedaços del producte. A part de la instal·lació dels pegats i l'actualització de les versions menors ("minor releases") que siguin necessaris per mantenir el producte en un nivell adequat i segur d'actualització, en el temps de durada del contracte, l'adjudicatari haurà de fer l'actualització de com a mínim una versió major del producte ("major release").
- Desenvolupament i posada en producció de nous serveis i funcionalitats; els evolutius per noves funcionalitats o millora de les existents és una tasca recurrent i rellevant en aquest servei i que ha de donar resposta i cobrir evolutius que de manera holística donen solucions a problemes o millores que es plantegen en la necessitat de l'Ajuntament de governar les identitats i accessos.
- Implementació de recomanacions de seguretat i prevenció d'incidents.
- Trasllat de la plataforma a un cloud gestionat per l'IMI.
- Les modificacions que afectin el servei hauran de realitzar-se fora de l'horari normal de prestació del servei.

- **Suport 12x5 per a la resolució d'incidències que no afectin el funcionament del sistema:**
  - Detecció, registre i diagnòstic d'incidències.
  - Resolució d'incidències notificades per l'Ajuntament.
  - Documentació de les activitats realitzades per a la resolució de les incidències.
  - Suport de nivell 2 als usuaris davant incidències relacionades amb la seva identitat. Atenció a l'usuari final quan sigui necessari per a la resolució d'incidències.
  - Dins del servei de suport s'inclou, a més:
    - Gestió de casos amb el fabricant per a la resolució d'incidències que així ho requereixin.
    - Accés il·limitat a les descàrregues de software, última versió del producte, pegats de seguretat i qualsevol altra actualització del producte.
    - Accés a documentació tècnica del producte.
    - Notificacions proactives de problemes de software conegut que permetin prendre mesures correctores.
- **Suport 24x7 pel personal que opera la solució de gestió d'identitats:**
  - Suport 24x7 per a la resolució d'aquelles incidències crítiques (afecten de manera global al sistema en producció i suposen una indisponibilitat total del sistema en producció) i urgents (incidències que afecten una funcionalitat principal) que afectin el funcionament del sistema.
  - Suport davant incidents de seguretat (ciberincidents) que requereixin dels serveis d'administradors del sistema de Gestió d'Identitats

- Suport davant de campanyes i operatives especials determinades per necessitats tècniques, operatives o de governança d'identitats i/o seguretat o d'altres serveis crítics vinculats a la gestió d'identitats (per exemple, campanyes de canvis de contrassenyes derivades d'un incident de seguretat, actualització d'un sistema vinculat com podria ser Active Directory...).
- Execució de RFCs que impactin en la disponibilitat total o parcial dels serveis i funcionalitats.

S'esperen, com a mínim, els següents lliurables:

- Informe de seguiment del servei.
- Informe de treballs realitzats.
- Informe d'incidències, peticions, etc.

4.5 EVOLUTIUS SOBRE LA PLATAFORMA ACTUAL DE GESTIÓ D'IDENTITATS (OIM)

Fins a la seva substitució per la nova eina, l'adjudicatari es farà càrrec del desenvolupament i desplegament d'evolutius funcionals sobre l'actual plataforma de gestió d'identitats basada en OIM, segons les necessitats definides per l'Ajuntament de Barcelona i per l'IMI.

4.6 FINALITZACIÓ DEL SERVEI I TRASPÀS DEL SERVEI

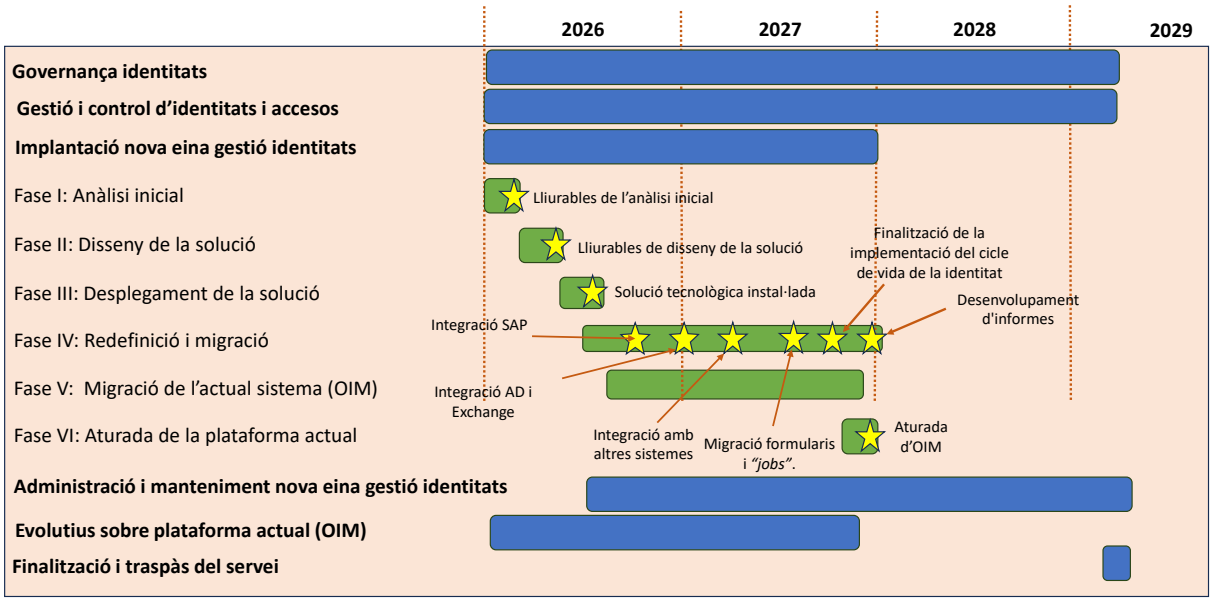
En aquesta fase es prepararà la finalització del servei i s'efectuarà una devolució ordenada del servei al personal de l'Ajuntament o a una altra empresa adjudicatària d'un futur concurs. Aquesta fase tindrà una durada d'**1 mes** i s'elaborarà, com a mínim, la següent documentació:

- Inventari d'actius.
- Descripció del model de dades implementat.
- Arquitectura desplegada.
- Descripció tècnica de les integracions configurades amb altres sistemes.
- Descripció de procediments o processos implementats.
- Manuals tècnics d'administració i operació.
- Manuals d'usuari.
- Informe amb els treballs pendents de realitzar, incidències i consultes pendents de resoldre.

4.7 PLANIFICACIÓ PROPOSADA

En el següent esquema es mostra una planificació orientativa per a l'execució del contracte, si bé, l'oferent pot proposar una altra planificació sempre que suposi una millora sobre la planificació mostrada.

Durant la migració haurà de conviure el nou sistema amb l'actual (OIM) i el seu desplegament no haurà de tenir impacte a l'Ajuntament de Barcelona.



Il·lustració 5. Planificació orientativa

5 EQUIP DE TREBALL

L'equip de treball proposat per l'adjudicatari haurà de comptar amb la suficient qualificació professional i disponibilitat per a la prestació del servei contractat, tot assegurant la seva estabilitat mentre estigui vigent el contracte.

Es pot requerir la presència en les instal·lacions de l'Ajuntament de Barcelona de com a mínim una part de l'equip de treball per a l'assistència a reunions de coordinació, anàlisi, comitès de seguiment, etc., així com per a la realització de les operacions tècniques quan sigui requerit per l'Institut Municipal d'Informàtica.

A continuació es descriuen les funcions, l'experiència i dimensionament de l'equip que l'Ajuntament de Barcelona considera que es necessiten, **com a mínim**; si bé podran o hauran de participar altres perfils en cas que es consideri necessari per al compliment dels objectius del contracte.

En qualsevol dels casos i en tot moment, l'adjudicatari haurà de complir els objectius del contracte i els requeriments definits al plec tècnic, i mai podrà justificar els incompliments en la manca de personal.

5.1 FUNCIONS

L'adjudicatari proposarà un equip de treball adequat per a l'execució de contracte. L'IMI estima que els perfils mínims necessaris a aportar per part de l'adjudicatari per a la prestació dels serveis d'aquest contracte són els que es llisten a continuació:

Perfil	Funcions
Responsable del contracte (R.C.)	• Gestionarà l'abast, les persones i organitzacions implicades, els riscos i els recursos necessaris, per tal de dur a terme el projecte i els serveis objecte del contracte sense desviacions. • Respondrà per l'empresa proveïdora davant l'IMI en qualsevol aspecte relatiu al contracte de prestació dels serveis. • Es responsabilitzarà de la planificació, gestió i control del servei i assegurarà la seva qualitat.
Cap de projecte	Responsable d'assegurar la correcta execució del projecte de desplegament de la nova solució i migració des de l'OIM (segons allò descrit a l'apartat 4.3). Màxim interlocutor amb el responsable del contracte i coordinador general de l'equip. En cas d'absència del responsable del contracte, les tasques seran subdelegades al perfil ara descrit. Entre les seves principals funcions destaca: • Garantir l'elaboració de tots els lliurables, manuals i informes de les fases I a IV (anàlisi inicial, disseny de la solució, desplegament de la nova solució i redefinició i migració).

	• Assegurar la correcta planificació, seguiment i control de les activitats del projecte. • Participar en els Comitès de Direcció i Seguiment. El cap de projecte haurà de comptar amb les habilitats de gestió necessàries per a aconseguir que les diferents fites marcades en la planificació s'aconsegueixin complint els requeriments de l'Ajuntament de Barcelona, així com tenir capacitat per a solucionar les incidències, identificar riscos i proposar solucions per a adaptar el projecte a les noves necessitats que sorgeixin durant la seva execució.
Coordinador del servei	Responsable d'assegurar l'operativa diària, definir, gestionar i executar les accions a realitzar en cadascun dels àmbits d'activitat del servei. Màxim interlocutor amb el responsable del contracte i coordinador general de l'equip. En cas d'absència del responsable del contracte, les tasques seran subdelegades al perfil ara descrit. Entre les seves principals funcions destaca: • Garantir l'elaboració de tots els lliurables, manuals i informes requerits als diferents serveis. • Assegurar el correcte funcionament dels serveis • Assegurar la correcta planificació, seguiment i control de les activitats. • Assegurar que els acompanyaments es realitzen correctament i d'acord als objectius planificats • Actualització dels indicadors i informes de seguiment del servei. • Assegurar la millora contínua del servei. • Participar en els Comitès de Direcció i Seguiment. • Garantir que els serveis de Transició s'executen adequadament.
Enginyer sènior en infraestructures de gestió d'identitats i control d'accés	Realitzarà les funcions d'analista funcional de cara a dissenyar la solució de gestió d'identitats.
Enginyers experts en la tecnologia proposada	• S'encarregaran de la instal·lació, configuració i administració de la tecnologia oferta. • Executaran les tasques necessàries per al desplegament de la tecnologia i la migració de la plataforma de gestió d'identitats. • Administració i suport de la nova eina de gestió d'identitats a mesura que es vagi completant la migració.

	• Implementaran els connectors i qualsevol altra funcionalitat que es determini en el marc de l'execució del projecte o durant la prestació dels serveis. • Activitats associades a la prestació dels serveis descrits als apartats 4.2, 4.4 i 4.5.
Consultor Sènior en Seguretat de la Informació	• Revisió i alineació de l'estratègia d'implantació amb les necessitats de la Direcció de Serveis de Seguretat de la Informació. • Anàlisi i disseny de noves arquitectures i funcionalitats. • Assegurament del compliment normatiu de la nova solució de gestió d'identitats.
Consultor sènior en governança d'identitats i control d'accés amb experiència com arquitecte d'identitats	Activitats associades a la prestació del servei de governança, descrit a l'apartat 4.1.

5.2 EXPERIÈNCIA I CONEIXEMENTS

Perfil	Experiència/Coneixements
Responsable del contracte (R.C.)	Cal que acrediti, durant els **darrers 5 anys**, una **experiència mínima** de **3 anys** en l'àmbit de la consultoria estratègica i/o projectes de transformació organitzativa. Haurà d'haver participat almenys en dos projectes com a responsable d'un servei de gestió del portafolis de projectes. Haurà de tenir coneixements de llengua catalana equivalent a nivell de suficiència C1
Cap de projecte	Cal que acrediti, durant els **darrers 8 anys**, una **experiència mínima** de **5 anys** en la direcció de projectes de gestió d'identitats i una **experiència mínima** de **5 anys** en projectes similars a l'objecte de la present licitació. Cal com a mínim acreditar **3 anys d'experiència** en models tradicionals com *PMBok*. Haurà de tenir coneixements de llengua catalana equivalent a nivell de suficiència C1

Coordinador del servei	Cal que acrediti, durant els **darrers 8 anys**, una **experiència mínima** de **5 anys** en la direcció de projectes de gestió d'identitats i una **experiència mínima** de **5 anys** en projectes similars a l'objecte de la present licitació. Cal com a mínim acreditar **3 anys d'experiència** en models com CMMI i ITIL. Haurà de tenir coneixements de llengua catalana equivalent a nivell de suficiència C1
Enginyer sènior en infraestructures de gestió d'identitats i control d'accés	Cal que acrediti, durant els **darrers 8 anys**, una **experiència mínima** de **5 anys** en la solució de gestió d'identitats proposada i una **experiència mínima** de **5 anys** en projectes similars a l'objecte de la present licitació.
Enginyers experts en la tecnologia proposada	Cal que acreditin, durant els **darrers 8 anys**, una **experiència mínima** de **5 anys** en la implantació i suport de solucions de gestió d'identitats i control d'accessos, **3 dels quals** en la solució de de gestió d'identitats proposada i una **experiència mínima** de **3 anys** en projectes similars a l'objecte de la present licitació. Hauran de disposar de coneixements i experiència amb l'eina de Gestió d'Identitats desplegada actualment (OIM). Hauran de disposar de coneixements tècnics sobre la infraestructura base que interactuarà amb el nou sistema de gestió d'identitats: Windows, Active Directory, Exchange, Linux, Oracle, LDAP, SAP, etc. Hauran de dominar la tecnologia oferta i disposar dels coneixements necessaris per a la implementació de les integracions amb els sistemes i els fluxos de treball. Hauran d'acreditar experiència en migració d'OIM a la tecnologia proposada, almenys en 1 projecte. Hauran d'estar certificats en la tecnologia oferta. Hauran de tenir coneixements de llengua catalana equivalent a nivell de suficiència C1
Consultor Sènior en Seguretat de la Informació	Cal que acrediti, durant els **darrers 8 anys**, una **experiència mínima** de **5 anys** en **projectes de seguretat de la informació** i **4 anys** en **projectes de gestió d'identitats**.
Consultor sènior en governança d'identitats i control d'accés amb experiència	Cal que acrediti, durant els **darrers 8 anys**, una **experiència mínima** de **7 anys** en **projectes de seguretat de la informació** i **4 anys** en projectes de gestió d'identitats.

com arquitecte d'identitats	Cal que acrediti, durant els **darrers 8 anys**, una **experiència mínima** de **7 anys** com a consultor en **projectes de governança d'identitats i control d'accessos** i com a arquitecte d'identitats i una **experiència mínima** de **4 anys** en **projectes** similars a l'objecte de la present licitació. Haurà de tenir coneixements de llengua catalana equivalent a nivell de suficiència C1.

5.3 DIMENSIONAMENT

S'han estimat les següents dedicacions mínimes dels equips assignats al contracte per part de les empreses licitadores:

Perfil	FTE fins al final de la migració de l'eina de gestió d'identitats	HORES ANUALS	FTE a partir del final de la migració de l'eina de gestió d'identitats	HORES ANUALS
Responsable de contracte	0,1	180	0,1	180
Cap de projecte	0,4	720	0,2	360
Coordinador del servei	0,2	360	0,4	720
Enginyer sènior en infraestructures de gestió d'identitats i control d'accés	0,1	180	0,1	180
Enginyers experts en la tecnologia proposada	2,6	4680	2,6	4680
Consultor Sènior en Seguretat de la Informació	0,1	180	0,1	180
Consultor sènior en governança d'identitats i control d'accés amb experiència com arquitecte d'identitats	1	1.800	1	1.800
TOTAL FTEs	4,5	8.100	4,5	8.100

Aquestes dedicacions mínimes s'han establert en base al coneixement i experiències prèvies en implantacions d'eines de gestió d'identitats de les persones tècniques responsables dels serveis de gestió d'identitats actuals.

5.4 MODEL DE GOVERN

Pel correcte seguiment del projecte i prestació dels serveis i la consecució de l'èxit en qualitat, terminis i homogeneïtat del treball a realitzar, s'estableix que el contracte estarà governat per 3 comitès:

- Comitè de Seguiment
- Comitè de Direcció
- Comitè de Crisi

L'acta de cada comitè/reunió haurà de ser enviades a l'IMI abans de **2 dies laborables** després de la seva realització.

5.5 COMITÈ DE SEGUIMENT

S'encarrega del dia a dia del projecte. Resol les incidències i conflictes menors que apareguin al llarg de la vida del projecte.

Es reunirà setmanalment durant les fases I a IV i quinzenalment a partir de la fase V. El responsable del contracte de l'IMI pot canviar la freqüència de les reunions quan ho consideri necessari per motius del servei. Està format com a mínim pel Responsable del contracte de l'adjudicatari, el cap de projecte de l'adjudicatari i el coordinador de servei de l'adjudicatari i el responsable del contracte de l'IMI. Quan calgui, es podrà convidar a les reunions del Comitè de Seguiment als membres de l'equip de projecte necessaris per tractar en profunditat determinats temes.

Amb caràcter obligatori, es convocarà una **reunió de Kick-off** o llançament de projecte amb els principals membres del projecte (Directors de l'IMI, Responsables de sector i transversals, Equip de l'adjudicatari i Equip IMI).

Li corresponen al Comitè de Seguiment les funcions de control de l'execució del contracte:

- Validació de la feina.
- Verificació de l'acompliment del contracte.
- Validació i aprovació de l'emissió de la factura corresponent als treballs realitzats.
- Verificació de l'acompliment dels ANS i del contracte.
- Resolució dels conflictes que puguin sorgir en l'execució del contracte.
- Presentació actualitzada de l'equip del servei i el percentatge de dedicació individual: és responsabilitat de l'adjudicatari presentar mensualment la totalitat de l'equip

participant en el servei, amb el percentatge de dedicacions individuals. Aquesta informació es creuarà amb la informació dels altres contractes actius que l'adjudicatari tingui amb l'IMI.

- Supervisió específica de la seguretat: Revisar periòdicament el compliment dels requeriments de seguretat establerts en el projecte, incloent-hi la gestió de riscos associats a les identitats i els accessos. Aquest punt inclou la verificació d'indicadors clau de seguretat (KPI) i l'anàlisi d'informes d'incidents o desviacions, així com la proposta de mesures correctives per garantir l'alineació amb les polítiques de seguretat de l'Ajuntament. Aquest aspecte serà tractat com a punt específic en les reunions del Comitè de Seguiment amb la participació, si escau, de representants de la Direcció de Serveis de Seguretat de la Informació.

Li correspon al responsable de l'empresa adjudicatària la preparació de la documentació necessària per a la realització del comitè de seguiment i aixecar acta dels temes i acords de la reunió.

El Responsable del contracte de l'adjudicatari és l'encarregat de fer les convocatòries i enviar la documentació necessària als participants com a mínim amb 3 dies laborables d'antelació, i d'aixecar acta de les reunions d'aquest Comitè.

5.6 COMITÈ DE DIRECCIÓ

Les seves funcions són les de supervisar la marxa del contracte i la presa de decisions que afecten a l'objectiu i abast del mateix.

Es reunirà amb caràcter mensual encara que l'IMI el podrà convocar amb caràcter extraordinari sempre que es consideri necessari. En formen part:

- Director/a de la Direcció de Tecnologia
- Cap de Departament designat per la direcció de la Direcció de Tecnologia
- Director de Seguretat o persona en qui delegui/Cap de Departament de Seguretat de la Informació.
- Responsable de contracte de l'IMI.
- Coordinador del contracte de l'adjudicatari.
- Altres assistents requerits.

Li corresponen al Comitè de Direcció les funcions de:

- Aprovar ampliacions/reduccions de contracte.
- Aprovar l'execució de les penalitzacions.
- Gestió de riscos i oportunitats.

Li correspon al responsable de l'empresa adjudicatària la preparació de la documentació necessària per a la realització del comitè de direcció i aixecar acta dels temes i acords de la reunió.

El Responsable del Servei de l'adjudicatari és l'encarregat de fer les convocatòries i enviar la documentació necessària als participants com a mínim amb 3 dies laborables d'antelació, i d'aixecar acta de les reunions d'aquest Comitè.

5.7 COMITÈ DE CRISI

En cas que l'IMI ho consideri necessari es podrà convocar un Comitè de Crisi. L'objectiu d'aquest comitè serà la posada en comú i solució d'una problemàtica o situació crítica.

La sol·licitud del Comitè de Crisi la realitzarà únicament l'IMI, qui establirà els assistents, l'hora i localització de la reunió, així com l'agenda i punts a tractar.

Aquest comitè es podrà convocar amb una antelació mínima de 4 hores a l'adjudicatari. El Comitè de Crisi s'anirà reunint amb la periodicitat que estableixi l'IMI mentre duri la contingència.

Li corresponen al Comitè de Crisi les funcions de:

- Analitzar el problema o situació i establir-ne la gravetat.
- Definir un pla de contingència per a la resolució immediata de la situació i fer seguiment.
- Definir un pla d'acció, si escau, per implantar mesures que impedeixen que el problema o situació torni a succeir i fer seguiment.
- Designar els responsables de l'execució de les accions definides.
- Designar els responsables encarregats de fer una investigació del succés i fer seguiment.
- Si fossin necessàries, definir les penalitzacions a aplicar sobre els responsables del succés.
- Establir les responsabilitats.

Li correspon al responsable de l'empresa adjudicatària la preparació de la documentació necessària per a la realització del Comitè de Crisi i aixecar acta dels temes i acords de la reunió.

6 REQUERIMENTS DE LA NOVA SOLUCIÓ DE GESTIÓ D'IDENTITATS

En aquest capítol s'indiquen els requeriments de la solució tecnològica i de la seva implementació que s'han de complir.

6.1 REQUERIMENTS D'INFRAESTRUCTURA (R.IN.)

- **R.IN.1**. El desplegament es realitzarà en dos entorns, "productiu" i "no productiu" de manera idèntica quant a arquitectura, versionat i configuració (cada entorn es troba en un centre de processament de dades diferent).

- **R.IN.2.** La solució haurà d'implantar-se en un entorn d'infraestructura com a servei (IaaS) o plataforma com a servei (PaaS) gestionat per l'Institut Municipal d'Informàtica (IMI), amb les següents condicions:
    - Per raons justificades, la solució es pot desplegar inicialment en servidors virtuals proporcionats per l'IMI o en la plataforma corporativa de gestió de contenidors de l'IMIperò s'haurà de contemplar un trasllat futur de la plataforma, de forma senzilla i amb un mínim impacte, cap a un cloud gestionat per l'IMI, en el moment que així ho indiqui l'IMI en funció de l'habilitació de l'entorn corresponent.
    - Per raons justificades, la solució es pot desplegar inicialment en servidors virtuals proporcionats per l'IMI o en la plataforma corporativa de gestió de contenidors de l'IMI. En aquests casos però, aquest desplegament inicial ha de preveure el trasllat, de forma senzilla i amb un mínim impacte, cap a un Cloud gestionat per l'IMI, en el moment que l'Institut ho determini i sempre i en tot cas abans de la finalització del contracte i en funció de l'habilitació de l'entorn corresponent.
    - La infraestructura haurà de garantir el control, la seguretat i el compliment normatiu establert per l'Ajuntament.
    - No s'admetran solucions que requereixen desplegar appliances físics al CPD municipal per a tota la funcionalitat del servei.

  així mateix la solució haurà d'estar preparada per a la integració amb serveis SaaS i arquitectures híbrides, facilitant així l'evolució cap a models cloud-native en el futur.
- **R.IN.3.** Tots els components hauran de desplegar-se en alta disponibilitat.
- **R.IN.4.** El sistema ha de ser escalable davant un augment del nombre d'identitats gestionades i/o per l'augment de sistemes integrats als quals s'aprovisionen comptes mitjançant connectors. L'Ajuntament adquirirà les noves llicències que fossin necessàries.
- **R.IN.5.** Es valorarà que el producte pugui ser instal·lat en contenidors (Kubernetes o altres).

6.2 REQUISITS DE LA SOLUCIÓ TECNOLÒGICA (R.TE.)

- **R.TE.1.** La tecnologia ha d'estar ben posicionada en informes de l'àmbit de Gestió i Governança de la Identitat dels últims anys emesos per consultores/analistes més rellevants.

- **R.TE.2.** El producte ha de proporcionar de manera nativa i amb el mínim desenvolupament de codi possible, totes les necessitats tècniques i funcionals detallades en aquest plec.

- **R.TE.3.** S'ha de poder personalitzar l'aspecte visual de la interfície dels usuaris. En particular, posar logotips corporatius i textos en l'idioma català.

- **R.TE.4.** El repositori d'identitats ha de suportar una estructura flexible de l'organització de l'Ajuntament, la qual, podrà evolucionar en el temps. Ha de permetre la incorporació de qualsevol nova dada que sigui necessari i gestionar qualsevol nou tipus d'identitat.

- **R.TE.5.** Els processos i components han d'estar basats en estàndards, com, per exemple, API REST, OAuth, SCIM, etc.

- **R.TE.6**. La informació emmagatzemada en el directori del sistema de gestió d'identitats ha de ser fàcilment consultables per les persones autoritzades i en funció del seu perfil.

- **R.TE.7.** L'eina ha de proporcionar un ampli catàleg de connectors, sent imprescindibles els següents: SAP (inclòs S/4HANA), Active Directory, Exchange, LDAP, bases de dades relacionals (JDBC), Entra ID i API Rest.

- **R.TE.8.** La configuració de polítiques per a la integració de sistemes ha de ser el més senzilla possible i nadiua en l'eina, tot minimitzant la necessitat d'haver de desenvolupar codi o scripts.

- **R.TE.9.** S'ha de poder afegir fàcilment la sincronització de nous camps des de la font mestra d'identitats (SAP) i la seva sincronització als restants sistemes.

- **R.TE.10.** Ha de suportar canvis massius en la informació d'identitats, tant en el propi sistema de gestió d'identitats, com en qualsevol dels sistemes integrats, sense que es produeixi una caiguda del sistema ni es vegi afectat el seu rendiment en altres processos de sincronització o interacció amb els usuaris.

- **R.TE.11.** En cas d'aturades programades o caigudes del sistema, quan el servei torni a estar disponible, ha de processar tots aquells canvis en les dades que s'hagin produït durant l'aturada i així garantir la correcta sincronització permanent de tota la informació.

- **R.TE.12.** Ha de proveir de serveis Web (API REST) per a la integració d'altres sistemes mitjançant anomenades als serveis Web proporcionats pel sistema de Gestió d'Identitats.

- **R.TE.13.** El repositori centralitzat d'informació ha d'assegurar la confidencialitat i integritat de la informació i impedir accessos no autoritzats.

- **R.TE.14.** El sistema ha de detectar comptes orfes en els sistemes o fallades en la sincronització de les dades i procedir a la seva reconciliació.

- **R.TE.15.** Ha d'implementar controls de seguretat d'accés als portals d'acord amb la política de seguretat corporativa.

- **R.TE.16**. Ha d'oferir funcionalitats de monitoratge que permetin conèixer l'estat del propi sistema i notificar mitjançant alertes, quan es detectin fallades en el seu funcionament. Per exemple, estat del directori, estat dels connectors amb els sistemes, etc.
- **R.TE.17**. La gestió de les identitats ha de poder realitzar-se de forma centralitzada (control total de les identitats), o mitjançant una gestió delegada, per exemple, sobre la base d'organismes o àrees de l'Ajuntament de Barcelona. Ha d'oferir la suficient flexibilitat com per a poder configurar les tasques que poden realitzar els usuaris en el sistema de gestió d'identitats i quines identitats poden gestionar.
- **R.TE.18.** Les identitats han de poder ser gestionades manualment per personal autoritzat amb el propòsit de poder realitzar les següents accions sobre la identitat de l'usuari:
    - Modificar qualsevol tipus d'informació emmagatzemada en la identitat.
    - Activar /desactivar el compte.
    - Modificar la contrasenya.
    - Modificar la data de caducitat dels comptes o de les contrasenyes.
- **R.TE.19.** S'ha de poder desenvolupar formularis per a l'aprovisionament manual d'identitats, rols, recursos, permisos, etc. per personal autoritzat i seguir un flux de treball establert d'aprovació o revocació.
- **R.TE.20.** Haver de proporcionar mecanismes que facilitin l'alta massiva d'identitats.
- **R.TE.21**. Ha de disposar d'un portal d'autoservei de contrasenya en el qual els usuaris puguin canviar la seva contrasenya.
- **R.TE.22.** Disposar d'un perfil del portal pel *"Help Desk"* per a l'equip del SAU que permeti restablir la contrasenya dels usuaris segons diferents mecanismes, entre ells, mitjançant la generació d'una clau d'un sol ús, així com poder visualitzar la informació dels comptes dels usuaris.
- **R.TE.23.** Ha de disposar d'un servei de cerca d'usuaris i consulta d'informació per personal autoritzat. S'ha de poder configurar els atributs que pot visualitzar l'usuari i qui pot visualitzar-lo.
- **R.TE.24.** Els usuaris han de poder modificar aquells atributs de la seva identitat sobre els quals tinguin autoritzat la seva modificació.
- **R.TE.25.** Ha de suportar la gestió de rols d'aplicacions i rols de negoci, així com la possibilitat que siguin assignats automàticament en funció de la informació dels atributs de les identitats.
- **R.TE.26.** Ha d'implementar controls de segregació de funcions (SoD) per incompatibilitats en sol·licituds en tràmit i en autoritzacions ja assignades.
- **R.TE.27.** Ha de proporcionar funcions de certificació de comptes i permisos en les quals es validi de manera periòdica l'assignació de rols o permisos. Ha de poder programar-se campanyes de certificació.

- **R.TE.28.** La plataforma de gestió d'identitats ha de mostrar l'històric del cicle de vida de la identitat, és a dir, totes aquelles modificacions que s'hagin anat realitzant i qui les ha realitzat, per exemple, quan va ser creada, quan se li ha estat assignat o eliminat un rol, quan es va modificar la contrasenya, aprovisionat a un sistema, etc.

- **R.TE.29.** La identitat ha d'incloure la relació de totes les credencials existents en els diferents sistemes, de manera que sigui possible establir la relació d'aquestes amb la identitat de l'usuari i poder bloquejar les credencials de manera immediata davant incidents de seguretat.

- **R.TE.30.** Ha de poder mostrar de manera fàcil els rols, permisos, recursos, etc. que tingui assignats l'usuari i poder revocar-los-hi de manera immediata davant incidents de seguretat.
- **R.TE.31.** Ha de poder establir fluxos de treball per als processos de sol·licituds, seguiment i aprovacions de rols, permisos o qualsevol altra entitat, així com emmagatzemar traces de tot el procés.
- **R.TE.32.** Ha d'identificar canvis no autoritzats en els sistemes integrats per a, posteriorment, desencadenar fluxos sobre aquests canvis: reconciliació, notificacions, certificacions, infraccions de polítiques de seguretat, etc.
- **R.TE.33.** Ha de registrar en un repositori local tota l'activitat realitzada en el sistema, canvis en les propietats de la identitat, fluxos de treball, etc. amb la finalitat de proporcionar evidències davant incidents de seguretat.
- **R.TE.34.** L'eina ha de poder realitzar exportacions de les dades de les identitats a fitxers (CSV, Excel, etc.) Ha d'oferir flexibilitat per a poder configurar les dades que s'han d'exportar i qui pot realitzar les exportacions. De manera controlada, sota autorització explícita i deixant evidències de les baixades. S'haurà d'integrar amb l'aplicatiu fet per aquest propòsit.
- **R.TE.35.** Ha d'integrar-se amb l'eina "Elastic" (ELK) com a repositori centralitzat de logs o el que sigui en aquell moment.
- **R.TE.36.** Els esdeveniments d'auditoria de la plataforma s'han d'integrar amb l'eina SIEM de l'Ajuntament IBM QRadar, o la que la substitueixi.
- **R.TE.37.** Totes les transmissions de dades hauran de configurar-se com a connexions segures, tant entre els propis components del sistema de gestió d'identitats com amb els sistemes integrats.
- **R.TE.38.** L'eina ha de permetre de forma àgil la gestió i el manteniment de les identitats d'usuaris externs, una a una i també amb accions massives. Ha de permetre operacions com la desactivació i la re-activació de l'usuari; l'establiment i modificació de la data de caducitat automàtica de l'usuari; la re-assignació del responsable intern de l'usuari; el forçat de contrasenya en el següent inici de sessió o el re establiment de la contrasenya; la consulta de totes les dades de l'usuari, incloent dades tècniques com últims accessos, 2FA enrolats, últims canvis de contrasenya...

6.3 REQUERIMENTS BÀSICS DEL DESPLEGAMENT (R.DE.)

- **R.DE.1.** Tota la *"interfície web"*, com a portals, formularis, missatges d'avís, etc. ha d'estar configurat en català.
- **R.DE.2.** S'han de desenvolupar formularis per a poder fer les següents tasques sobre els usuaris i només podran ser iniciats per personal autoritzat:
    - Canvi de tipologia d'usuari (d'extern a intern).
    - Pre-alta d'usuaris interns.
    - Alta d'usuaris interns sense nòmina en SAP (usuaris T3) i externs (usuaris T4).
    - Alta d'usuaris genèrics (G1) i de servei (S1).
    - Modificació de dades de l'usuari.
    - Reactivar una identitat tot assignant-li una nova organització.
    - Desactivar una identitat.
    - Deshabilitació administrativa d'una identitat.
    - Reactivació d'una identitat de l'estat de *"deshabilitació administrativa"*.
    - Sol·licitud d'assignació / revocació del recurs de correu corporatiu per usuaris que no tenen el correu corporatiu per defecte.
    - Sol·licitud d'assignació / revocació de compte amb privilegis en Active Directory.
- **R.DE.3.** S'ha de desplegar un portal d'autoservei de contrasenyes perquè els usuaris puguin modificar la seva contrasenya i restablir-la en cas d'oblit. Aquest portal s'haurà d'integrar o complementar amb el PAC, o substituir-lo. El PAC (*Portal d'Autogestió de la Contrasenya*) és l'actual portal d'autoservei de contrasenyes desplegat a internet i protegit amb els 2FA corporatius.
- **R.DE.4.** S'ha d'implementar la funcionalitat de cerca d'usuaris per personal autoritzat, així com la modificació pels propis usuaris de la informació que s'autoritzi.
- **R.DE.5.** Proporcionar un servei per a facilitar la gestió dels usuaris personals i els comptes de genèriques i comptes de servei.
- **R.DE.6.** S'ha d'integrar amb el sistema de monitoratge i qualitat del servei de l'IMI

6.4 REQUERIMENTS DEL CICLE DE VIDA DE LA IDENTITAT (R.CV.)

- **R.CV.1.** S'ha de configurar una política per tal d'establir l'identificador d'usuari i l'àlies del seu correu electrònic corporatiu segons la lògica implementada actualment.
- **R.CV.2.** La gestió de les identitats (alta, baixa i modificació) pot ser tant des de font autoritzativa (ex. SAP) com des del propi sistema de gestió d'identitats per les entitats no sotmeses a nòmina.
- **R.CV.3.** L'aprovisionament i desaprovisionament de la identitat s'ha de poder realitzar en funció de la ubicació departamental de la identitat.

- **R.CV.4.** Ha d'existir un estat de "PREALTA" que permeti anticipar l'alta d'usuaris interns abans que es produeixi la seva alta en la font mestra d'identitats. Aquest estat crearà la identitat en els sistemes d'informació, previ a l'alta en SAP HR per tal de permetre accés als sistemes d'informació de l'Ajuntament fins que sigui donat d'alta en l'eina SAP de Recursos Humans.
- **R.CV.5.** Ha d'existir un estat de "deshabilitació administrativa" que permeti desactivar la identitat i els seus comptes associats per qualsevol motiu (seguretat, compliment, etc.) Aquest estat deshabilitarà els accessos als sistemes d'informació integrats, i no podrà modificar-se per les fonts mestres corresponents. Només es podrà tornar a activar la identitat de manera manual en el sistema de gestió d'identitats.
- **R.CV.6.** Les identitats poden trobar-se en tres estats per a tots els col·lectius (al marge de l'estat de pre-alta o altres subestats associats a la baixa, com actualment podrien ser notexist o lopd):
    - Actiu: la identitat està prestant servei a l'Ajuntament.
    - Inactiu: La identitat ha deixat de prestar serveis recentment.
    - Baixa: quan una identitat porta més temps sense prestar servei a l'Ajuntament.
- **R.CV.7.** Per als usuaris on la font mestra no és SAP (interns sense nòmina gestionada en SAP, externs, genèrics i de servei):
    - Ha d'existir una data d'inactivació de la identitat que no pot ser superior a un any respecte a la data d'alta de l'usuari.
    - Tant els propis usuaris com el seu responsable han de rebre una notificació uns dies abans de la data d'inactivació tot indicant que, si l'usuari ha de continuar actiu, ha de renovar-se.
    - En cas que arribi la data d'inactivació de la identitat i no s'hagi renovat, aquesta identitat ha de passar a estar inactiu.
- **R.CV.8.**. Per als usuaris on la font mestra és SAP, quan arriba una baixa des d'aquesta font mestra, ha d'aplicar-se una data final de vigència. A partir d'aquesta data, la identitat passarà a estat "inactiu" i s'establirà una nova contrasenya.
- **R.CV.9.** Per a totes les tipologies d'identitat, quan passen a estat inactiu, ha de calcular-se una data de baixa definitiva uns mesos després del pas a inactiu (actualment 6 mesos).
- **R.CV.10.** S'ha de contemplar la possibilitat de reactivar identitats – cas bastant habitual en la gestió de VIPs i durant els canvis de mandat, actualment als VIPs durant els primers 15 dies en estat inactiu se'ls manté l'accés a una sèrie de recursos i en un segon període de 15 dies se'ls treuen de forma automàtica.
- **R.CV.11.** Quan arribi la data de baixa definitiva de la identitat, aquesta ha de moure's a estat de baixa, s'eliminaran tots els seus permisos i s'establirà una nova contrasenya.
- **R.CV.12.** Per norma general, la relació entre els estats de la identitat i l'estat dels comptes d'informació aprovisionades a la identitat ha de ser:

- Pre-alta: previ a l'alta es crea compte desactivat en els sistemes finals amb les autoritzacions assignades per accedir als sistemes d'informació de l'Ajuntament fins que sigui donat d'alta en SAP HR.
- Actiu: comptes activats en els sistemes finals i amb les autoritzacions assignades.
- Inactiu: comptes desactivats en els sistemes finals. En funció de com s'hagin assignat les autoritzacions:
  - Autoritzacions assignades des del sistema de gestió d'identitats: s'eliminaran les autoritzacions.
  - Autoritzacions assignades directament en el sistema final: es mantindran assignades durant un període de cortesia (malgrat estar deshabilitat l'accés). Passat aquest període, s'eliminaran les autoritzacions.
- Deshabilitació administrativa: comptes desactivats en els sistemes finals, però amb les autoritzacions assignades.
- Baixa: comptes eliminats en els sistemes finals amb les seves autoritzacions.

- **R.CV.13.** Per als usuaris externs, s'ha de detectar aquells que porten un període determinat sense activitat i notificar als seus responsables aquesta situació, per a poder gestionar la baixa corresponent.
- **R.CV.14** El sistema gestió d'identitats ha de gestionar una data de caducitat del compte d'usuari. Quan s'aproximi la data de caducitat, ha d'enviar automàticament un correu informant de tal circumstància. Una vegada aconseguida aquesta data, el compte de l'usuari serà deshabilitat en el directori corporatiu i eliminat o deshabilitat en tots aquells sistemes de l'Ajuntament en els quals hagi estat aprovisionat el seu compte.
- **R.CV.15.** S'implementarà una gestió del cicle de vida per a comptes genèrics i comptes de servei. Regularment s'haurà d'enviar una notificació al seu responsable per a verificar que aquest compte continua sent necessari.
- **R.CV.16.** S'ha de donar continuïtat a la funcionalitat de l'actual portal de gestió d'usuaris subordinats (GIDExt), que permet als usuaris interns tenir control i gestionar, de manera autònoma, fàcil i àgil, els usuaris que tenen al seu càrrec (usuaris externs, de servei i genèrics). En la nova eina/servei s'haurà de disposar com a mínim de totes les funcionalitats que aporta aquest portal GIDExt, i d'altres de relacionades que s'identifiquin durant el projecte de posada en marxa de la nova eina de gestió d'identitats.

6.5 REQUISITS D'ADMINISTRACIÓ DELEGADA (R.AD.)

- **R.AD.1.** El sistema ha de permetre diferents nivells d'administració.
- **R.AD.2.** S'ha d'implementar un rol d'administració que permeti als referents d'usuaris interns sense nòmina (T3) sol·licitar l'alta d'aquesta tipologia d'usuaris.
- **R.AD.3.** S'ha d'implementar un rol d'administració que permeti als referents d'usuaris externs (T4) sol·licitar l'alta d'aquesta tipologia d'usuaris.
- **R.AD.4.** Els usuaris gestionats per administració delegada (T3 i T4) només han de poder situar-se a nivell d'estructura organitzativa per sota del peticionari / referent.
- **R.AD.5.** Els referents d'usuaris han de ser capaços de:

- Poder llistar als usuaris dels quals són responsables i ordenar-los per uns certs camps (per exemple, la data de pròxima inactivitat, la data del darrer accés,...).
- Modificar les principals dades dels usuaris T3, T4, G1 i S1.
- Assignar-los a un nou referent.

- **R.AD.6.** S'ha d'implementar un rol de *"Help Desk"* a assignar al personal de SAU que permeti la cerca d'usuaris, visualització de la informació dels usuaris, canvi de la seva contrasenya, etc.

6.6 REQUISITS DELS FLUXOS DE PETICIONS (R.FP.)

- **R.FP.1.** S'ha d'implementar un flux amb participació en l'autorització per part de Seguretat per a demanar comptes d'administració en el Active Directory.
- **R.FP.2.** S'ha d'implementar un flux amb aprovació per a sol·licitar un compte de correu de l'Ajuntament per identitats a les quals no se'ls assigna per defecte.
- **R.FP.3.** S'ha d'implementar un flux amb aprovació per a sol·licitar l'alta d'identitats genèriques o de servei.
- **R.FP.4**. Ha de permetre's la implementació de manera senzilla de fluxos amb aprovació d'autoritzacions a aplicacions per part dels referents de negoci.

6.7 REQUERIMENTS DE LES CONTRASENYES (R.CO.)

- **R.CO.1.** Tot canvi de contrasenya en els sistemes TIC de l'Ajuntament que l'IMI consideri, se sincronitzarà amb el sistema de gestió d'identitats.
- **R.CO.2.** S'ha d'implementar la política de contrasenyes corporativa quant a complexitat, caducitat i històric de la contrasenya per a cadascun dels col·lectius.
- **R.CO.3.** L'exclusió de la política de caducitat per als usuaris genèrics o de servei ha de comportar una excepció de seguretat amb participació en l'autorització del Direcció de Serveis de Seguretat de la Informació.
- **R.CO.4.** Els comptes han de tenir una data de caducitat de la contrasenya i el sistema de Gestió d'Identitats ha d'informar l'usuari de la pròxima caducitat de la seva contrasenya. En cas de superar aquesta data, es procedirà a inhabilitar el compte en el sistema de gestió d'identitats i en els sistemes integrats.
- **R.CO.5.** La contrasenya inicial de qualsevol tipus usuari ha de lliurar-se expirada, és a dir, ha de forçar-se el canvi en el seu primer ús.
- **R.CO.6.** El lliurament de la contrasenya inicial de qualsevol tipus d'usuari ha de realitzar-se d'acord amb el que s'estableix pel Direcció de Serveis de Seguretat de la Informació.
- **R.CO.7.** Quan es faci un canvi administratiu de la contrasenya (via SAU, administradors de l'eina de gestió d'identitats, etc.) aquesta ha de generar-se expirada, és a dir, ha de forçar-se el canvi en el seu primer ús.

6.8 REQUERIMENTS D'INTEGRACIÓ AMB ALTRES SISTEMES (R.IS.)

- **R.IS.1.** La solució s'ha d'integrar amb:

- Sistema SAP HR com a font mestra per a l'aprovisionament d'usuaris interns amb nòmina (T1 i T11). La integració es realitzarà de manera nativa.
- Sistema SAP HR per a l'aprovisionament de l'estructura organitzativa de l'Ajuntament de Barcelona.
- Sistema SAP HR per a aprovisionar dades des de gestió d'identitats, com l'identificador d'usuari, telèfon i l'adreça de correu electrònic.
- Sistema SAP CUA per a la gestió de comptes d'usuari dels diferents sistemes SAP de l'Ajuntament de Barcelona.
- Active Directory corporatiu.
- Sistema de correu corporatiu (Exchange).
- Base de dades d'autoritzacions (Control User).
- Repositoris LDAP d'autoritzacions corporatives.
- Repositori d'usuaris de GetAccess.
- Els següents sistemes d'autenticació multifactor: Cisco DUO, Google Authenticator i Microsoft Authenticator.

- **R.IS.2.** La integració amb els diferents sistemes ha de cobrir les següents funcionalitats:
  - Creació de comptes.
  - Modificació de comptes.
  - Sincronització de la contrasenya.
  - Esborrament de comptes.
  - Activació / Desactivació de comptes.
  - Assignació / Revocació d'autoritzacions.
  - Reconciliació de comptes i autoritzacions.
  - Descobriment de comptes orfes.
- **R.IS.3.** La sincronització dels canvis en la informació de les identitats des del sistema de gestió d'identitats als sistemes (ex. un canvi de la contrasenya d'un usuari o l'eliminació de permisos o bloqueig d'una identitat), ha de ser inferior a 10 segons, excepte que es tracti de sistemes en els quals es planifiqui el moment en el qual realitzar la sincronització de les dades o s'estableixi una freqüència de sincronització.

6.9 REQUERIMENTS D'AUDITORIA I INFORMES (R.AI.)

- **R.AI.1.** Ha de disposar d'un sistema flexible per al desenvolupament d'informes sense necessitat de desenvolupar codi. Ha d'incloure informes predefinits i tenir la capacitat de desenvolupar nous informes i programar la seva execució.
- **R.AI.2.** S'han de generar informes sobre volumetries d'identitats sobre la base de l'estat, tipologia, estat de la contrasenya (caducada, vigent, etc.)

- **R.AI.3.** S'han de generar informes sobre volumetries de comptes d'identitats en sistemes, estat dels comptes, comptes orfes, etc.
- **R.AI.4.** S'han de generar informes sobre rols de negoci i polítiques d'accés, criticitat dels drets d'accés gestionats, etc.
- **R.AI.5** S'han de generar informes sobre processos de compliment, com a processos de certificació de drets completats, escenaris de segregació de funcions, etc.
- **R.AI.6.** S'han de generar informes sobre identitats amb alts riscos de seguretat, tot detectant diferents motius: permisos crítics gestionats directament en el sistema final, permisos d'administració, etc.
- **R.AI.7.** S'ha de guardar registre de totes les activitats i canvis realitzats sobre les identitats, fluxos de treball, gestió de contrasenyes, accessos al sistema, etc. Aquests registres també han de guardar-se en el repositori centralitzat de logs *"Elastic"*.
- **R.AI.8.** S'ha de guardar registre dels canvis de configuració realitzats en el sistema de gestió d'identitats. Aquests registres també han de guardar-se en el repositori centralitzat de logs *"Elastic"*.

6.10 REQUERIMENTS DE COMPLIMENT (R.CU).

- **R.CU.1.** S'han d'implementar fluxos de certificació perquè el referent d'una identitat revisi i validi periòdicament, almenys, les autoritzacions crítiques (amb major risc) d'una identitat.
- **R.CU.2.** S'han d'implementar fluxos de segregació de funcions per a detectar anomalies d'assignació d'autoritzacions entre permisos incompatibles entre si.

7 ACORDS DE NIVELL DE SERVEI / COMPLIMENT DE FITES

7.1 COMPLIMENT DE FITES DEL PROJECTE D'IMPLANTACIÓ/MIGRACIÓ

En l'oferta es presentarà la planificació del projecte, on s'indicaran les dates previstes de les següents fites:

- Finalització de la fase I d'anàlisi de la solució.
- Finalització de la fase II de disseny de la solució.
- Data de finalització del desplegament de la tecnologia.
- Data d'implementació dels connectors amb SAP.
- Data d'implementació dels connectors amb Active Directory i Exchange.
- Data d'implementació dels connectors Control User, OUD i OES.
- Data de migració dels formularis per a l'aprovisionament manual de les identitats.
- Data d'implementació del cicle de vida de les identitats.
- Data d'implementació del portal d'autoservei de contrasenyes.
- Data de parada d'Oracle Identity Manager.

Es considera que s'ha complert amb la fita quan s'hagi estat aprovat pel responsable del projecte designat per l'Ajuntament de Barcelona.

Per a mesurar la desviació del compliment de la fita s'utilitzarà la següent fórmula:

Percentatge de desviació = 100 * (durada real de la fita – durada prevista) / durada prevista de la fita

No s'inclourà en el període de durada real de la fita, aquells retards que hagin estat causats per l'Ajuntament de Barcelona.

En cas que es produeixin desviaments en les dates de compliment de les fites, s'aplicaran les següents penalitzacions en la facturació associada al compliment de la fita:

- Entre 10% i 25% penalització d'un 1%.
- Entre més de 25 i fins a 50% penalització d'un 5%.
- Més d'un 50%, penalització d'un 10%.

En el cas del servei de governança d'identitats s'hauran d'elaborar els següents informes sobre l'estat de govern d'identitats a l'Ajuntament de Barcelona.

- Informe preliminar de l'estat de governança d'identitats.
- Informe de l'estat de governança d'identitats als 12 mesos de l'inici del projecte.
- Informe de l'estat de governança d'identitats als 24 mesos de l'inici del projecte.
- Informe de l'estat de governança d'identitats a la finalització del contracte (als 30 mesos des de l'inici del projecte).

En cas que es produeixin desviaments en la data de lliurament de la documentació associada a la consultoria, s'aplicaran les següents penalitzacions:

- Lliurament de l'informe entre 11 i 15 dies laborables des de de la data planificada tindrà una penalització d'un 2% de l'import dels serveis de governança de la següent factura.
- Lliurament de l'informe amb més de 15 dies laborables des de la data planificada tindrà una penalització d'un 5% de l'import dels serveis de governança de la següent factura.

L'equip del servei de governança d'identitats haurà d'assistir a totes aquelles reunions que se li sol·licitin per tenir relació amb la Governança d'Identitats; en cas de no assistència a les reunions a les quals se li convoqui s'aplicaran les següents penalitzacions:

- Falta d'assistència a les reunions a les quals es convoqui superior a un 5%, penalització d'un 2% de l'import dels serveis de governança següent factura.

7.2 OPERACIÓ I ADMINISTRACIÓ DE LA NOVA EINA DE GESTIÓ D'IDENTITATS I ACCESSOS

El nivells de servei descrits en aquest apartat es començaran a aplicar després de la finalització de la fase III del projecte d'implantació de la nova eina (*"Desplegament de la nova solució de gestió d'identitats")* i fins a la finalització del contracte.

7.2.1 Temps de resposta i resolució d'incidències

L'horari del servei es prestarà de dilluns a divendres de 08.00 a 20.00 no festius a Barcelona ciutat. Durant aquest horari de servei, la notificació d'incidències es realitzarà a través de la plataforma de tiquets *"EasyVista "* proporcionada per l'Ajuntament de Barcelona.

Fora d'aquest horari s'haurà de poder contactar 24x7 amb l'equip que administra la plataforma per a la resolució d'incidents que afectin el funcionament de la tecnologia o processos implementats o bé, per incidents de seguretat que poguessin necessitar del suport de l'equip de Gestió d'Identitats.

S'estableix el següent nivell de servei per a la resposta davant incidències:

Categoria de la incidència	Criteri de classificació de la categoria	Temps de resposta	Temps de resolució
Crítica	Afecten de manera global al sistema en producció i suposen una indisponibilitat total del sistema en producció.	1 hora laborable	3 hores en horari 24x7
Urgent	Incidències que afecten una funcionalitat principal.	1,5 hores laborables	6 hores en horari 24x7
Important	Incidències que afecten una funcionalitat secundaria.	4 hores laborables	3 dies laborables
Baixa	Incidències que no afecten l'operativa normal.	8 hores laborables	6 dies laborables

Taula 1. Temps de resposta davant incidents

El percentatge de compliment del temps de resposta i de resolució de les incidències ha de ser superior al 95%, tot aplicant una penalització del 5% en la factura corresponent a la "administració i suport de la nova solució" cas que no s'assoleixi un compliment del 95%.

El temps de resolució es calcularà des del moment del seu registre del tiquet per part del SAU i assignació a l'adjudicatari fins a la total resolució del mateix, incloent-hi les possibles reobertures i tancaments no definitius.

7.2.2 Temps de resposta PETICIONS DE SERVEI I ACTUALITZACIÓ DE PROBLEMES

Durant l'horari de servei, a més de resoldre les incidències en base al que s'ha indicat en l'apartat anterior, caldrà resoldre les peticions que es rebin a través de la mateixa plataforma "Easyvista" i documentar els problemes (causes o possibles causes d'un o varis incidents).

S'estableix el següent nivell de servei per a la gestió de peticions de servei i actualització de problemes:

Activitat	Descripció	Criticitat Ordinària	Criticitat Alta
Temps d'actualització dels problemes	Freqüència en què s'actualitza l'estat dels problemes	<= 5 dies laborables	<= 5 dies laborables

Temps de resolució de peticions ordinàries	Temps que transcorre entre la comunicació d'una petició ordinària i la resolució efectiva d'aquesta	<= 48 hores	<= 24 hores

Taula 2. Temps de resposta peticions de servei i actualització de problemes

El temps de resolució es calcularà des del moment del seu registre del tiquet per part del SAU i assignació a l'adjudicatari fins a la total resolució del mateix, incloent-hi les possibles reobertures i tancaments no definitius.

7.2.3 Reobertura de tiquets

Una altra mètrica rellevant que cal assegurar és la reobertura de tiquets d'incidències, considerem que per donar un bon servei aquest volum ha de ser ínfim i per tant s'estableix el següent nivell de servei per a la reobertura de tiquets:

Nom	Descripció	Fòrmula de càlcul	Periodicitat	Valor
Volum de tiquets reoberts	Nº tiquets reoberts per incorrecta resolució.	Incidències reobertes/ incidències tancades	Mensual	<=5%

Taula 3. Volum de tiquets reoberts

El percentatge de compliment d'aquest acord de servei és que sigui inferior al 5%, avaluant-se e forma mensual, és a dir, el nombre de tiquets reoberts en un mes natural no pot representar més del 5% del total de tiquets d'incidències tancades en aquell mes; en cas que no s'acompleixi aquest acord de nivell de servei algun mes des de l'inici d'algun dels serveis del contracte s'aplicarà una penalització del 10% en la següent factura corresponent a la prestació del servei de gestió d'identitats i accessos (operació i gestió continuada) i governança d'identitats.

8 DOCUMENTACIÓ TÈCNICA I ECONÒMICA DE L'OFERTA I FACTURACIÓ

8.1 PROPOSTA TÈCNICA (CONTINGUT SOBRE ELECTRÒNIC B)

El licitador haurà de presentar al sobre electrònic B, que serà la font per valorar els criteris subjectius, la seva oferta en format electrònic, on tots els arxius han d'estar en format Word, Excel, Power Point, MSProject o Acrobat.

El licitador podrà adjuntar tota la informació complementària que consideri d'interès, si bé, haurà de presentar els següents continguts mínims i estar obligatòriament estructurat de la manera següent:

- Identificació de l'oferta i dades de contacte.
- Acceptació de les condicions del plec. Declaració explícita d'acceptació de les condicions i requisits del plec amb les precisions que fossin necessàries.
- Descripció breu de l'oferta amb un resum executiu amb el més destacat de l'oferta (màxim cinc pàgines).
- Producte / Tecnologia proposada de Gestió d'Identitats amb el seu model de llicenciament i suport per part del fabricant (només es pot oferir una única solució tecnològica).
- Descripció detallada de l'oferta, on s'haurà d'indicar:
    - Arquitectura plantejada.
    - Disseny de la solució.
    - Estratègia de migració.
    - Detall de les tasques a realitzar per a la migració del sistema de gestió d'identitats a la nova tecnologia.
    - Implantació dels processos.
    - Aproximació a la gestió del cicle de vida de les identitats.
    - Adequació als requeriments establerts.
- Planificació del projecte:
    - Descripció de les fases, fites amb les seves dates i lliurables. Haurà d'especificar-se la data prevista de compliment de les següents fites:
        - Finalització de la fase I d'anàlisi de la solució.
        - Finalització de la fase II de disseny de la solució.
        - Data de finalització del desplegament de la tecnologia.
        - Data d'implementació dels connectors amb SAP (aprovisionament de les identitats des de les fonts mestres).
        - Data d'implementació dels connectors amb Active Directory i Exchange.
        - Data d'implementació dels connectors Control User, OUD i OES.

  - Data de migració dels formularis per a l'aprovisionament manual de les identitats
  - Data d'implementació del cicle de vida de les identitats.
  - Data d'implementació del portal d'autoservei de contrasenyes.
  - Data d'aturada d'Oracle Identity Manager.
- Metodologia de gestió del projecte.
- Proposta de lliurables.
- Pla de qualitat.
- Pla de devolució del servei.
- Recursos tècnics i humans. Personal proposat, perfils, dedicació, etc.
- Seguretat : clàusules, compromisos i mesures destinades a garantir la seguretat i confidencialitat de la informació.
- Referències: referències de l'empresa, del producte tecnològic, dels professionals, etc.
- Una altra informació que el licitador consideri d'interès.

Els licitadors hauran d'aportar una declaració responsable que acrediti que disposen de l'equip professional requerit i que ho posaran a la disposició de l'execució del contracte en cas de resultar adjudicataris.

La documentació presentada no ha de superar les 30 pàgines i ha de donar resposta, amb termes senzills i no subjectes a interpretació, al que es sol·licita en aquest plec tècnic; de cara a les valoracions s'exclourà tota aquella informació que no sigui clarament mapejable als criteris de valoració. En relació als criteris d'adjudicació sotmesos a judicis de valor únicament es valorarà la informació aportada en la documentació presentada amb el límit anterior (30 pàgines).

8.2 PROPOSTA ECONÒMICA (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 avaluables de forma automàtica, assenyalats en el plec de clàusules administratives particulars que regeix aquesta contractació, així com qualssevol altra documentació que aquest estableixi.

Els licitadors presentaran al sobre C la seva oferta econòmica (IVA exclòs) tot incloent el desglossament de les següents partides:

8.3 FACTURACIÓ

L'adjudicatari realitzarà la següent facturació sobre la base del compliment de les fites del pla de treball descrit en el capítol 4.7.

Factura	Fita	Import facturable dels serveis
1	Finalització de l'anàlisi inicial (mes 1 des de l'inici del contracte)	3% del cost dels serveis professionals associats a anàlisi, disseny, instal·lació de producte i migració des d'OIM (42% dels costos dels serveis professionals)
2	Finalització del disseny de la solució (mes 2 des de l'inici del contracte)	3% del cost dels serveis professionals associats a anàlisi, disseny, instal·lació de producte i migració des d'OIM (42% dels costos dels serveis)
3	Finalització del desplegament de la nova solució (mes 3 des de l'inici del contracte)	4% del cost dels serveis professionals associats a anàlisi, disseny, instal·lació d producte i migració des d'OIM (42% dels costos dels serveis professionals)
4	Redefinició i migració del sistema actual de gestió d'identitats: Finalització de la integració amb SAP (màxim mes 6 des de l'inici del contracte)	7% del cost dels serveis professionals associats a anàlisi, disseny, instal·lació d producte i migració des d'OIM (42% dels costos dels serveis professionals)
5	Redefinició i migració del sistema actual de gestió d'identitats: Finalització de la integració amb Active Directory i Exchange (màxim mes 9 des de l'inici del contracte).	5% del cost dels serveis professionals associats a anàlisi, disseny, instal·lació d producte i migració des d'OIM(42% dels costos dels serveis professionals)
6	Redefinició i migració del sistema actual de gestió d'identitats: Finalització de la integració amb la resta dels sistemes (connectors) (màxim 21 des de l'inici del contracte).	5% del cost dels serveis professionals associats a anàlisi, disseny, instal·lació d producte i migració des d'OIM (42% dels costos dels serveis professionals)
7	Implementació del portal d'autoservei (màxim mes 21 des de l'inici del contracte).	5% del cost dels serveis professionals associats a anàlisi, disseny, instal·lació d producte i migració des d'OIM (42% dels costos dels serveis professionals)
8	Implementació del cicle de vida de la identitat (aturada d'OIM) (màxim mes 21 des de l'inici del contracte).	10% del cost dels serveis professionals associats a anàlisi, disseny, instal·lació d producte i migració des d'OIM (42% dels costos dels serveis professionals)
9	Prestació del servei de gestió d'identitats i accessos (operació i gestió continuada) i governança d'identitats (a partir de la finalització del desplegament de la solució prevista pel mes 3 des de l'inici del contracte)	58% dels serveis professionals associats a l'operació i gestió continuada de la nova eina i a la governança d'identitats. Es facturarà proporcionalment de manera bimestral lligat al compliment dels ANS descrits a l'apartat 7 des de l'inici de la prestació d'aquests serveis – a partir de la finalització de la integració amb SAP - fins a la finalització del contracte.

Taula 4. Facturació dels serveis del projecte

S'entén que qualsevol fita és aconseguida quan hagi estat validada i formalment acceptada per part del cap de Projecte de l'Ajuntament de Barcelona mitjançant una acta d'acceptació.

L'adjudicatari realitzarà la següent facturació corresponent al subministrament de les llicències necessàries i servei de suport per part del fabricant al mes de desembre de cadascun dels anys de contracte:

Factura	Import facturable de les llicències i suport del fabricant
10	Cost de llicències i suport del fabricant pels mesos transcorreguts des del desplegament de la solució tecnològica (eina instal·lada, mes 3 de l'inici del contracte) fins al final de l'any corresponent (màxim 7 mesos).
11	Cost de llicències i suport del fabricant pels 12 mesos, corresponent a l'any següent del contracte.
12	Cost de llicències i suport del fabricant pels 12 mesos, corresponent a l'any següent del contracte
13	Cost de llicències i suport del fabricant pels mesos restants de la diferència entre 34 mesos i la suma dels mesos facturats a les factures 10, 11 i 12 (romanent final).

Taula 5. Facturació de les llicències del producte i suport del fabricant.

9 CLÀUSULES GENERALS

9.1 ACREDITACIONS I ACCEPTACIÓ DE CONDICIONS I REQUERIMENTS

Els licitadors hauran d'estar en possessió de quantes certificacions, autoritzacions, llicències i permisos siguin exigibles per la legislació vigent per a l'execució dels serveis i subministraments oferts.

El Plec Tècnic i els seus annexos revesteixen caràcter contractual, per la qual cosa la presentació d'ofertes implica manifestació expressa del licitador que accepta el seu contingut i conformitat amb aquests, havent de ser signats en prova de la seva acceptació, per l'adjudicatari en l'acte mateix de la formalització del contracte.

9.2 COMPLIMENT DELS PROCEDIMENTS I ESTÀNDARDS DE L'IMI I GESTIÓ DEL CANVI

En la prestació del servei de gestió d'identitats i accessos descrit en el plec, s'haurà de fer acompliment amb els procediments d'operació de l'Institut Municipal d'Informàtica.

S'hauran de realitzar no tan sols tasques tècniques sinó les d'acompanyament, gestió del canvi, divulgació, formació a usuaris finals (RRHH, T3, referents), confecció de manuals, formació al SAU (resolució d'incidències, traspàs d'operatives, documentació d'operatives diàries i funcionalitats puntuals, operacions massives sobre identitats), proveir indicadors i implementació de peticions associades a identitats al portal d'autoservei.

Qualsevol canvi que afecti la tecnologia de gestió d'identitats s'haurà d'implementar primer en l'entorn *"no productiu"* per tal de verificar el seu correcte funcionament. Els canvis que tinguin impacte en el servei hauran de realitzar-se fora de l'horari laboral.

9.3 LOCALITZACIÓ DE LA PRESTACIÓ DELS SERVEIS I DE L'EQUIP DE PROJECTE

Els serveis objecte del contracte es prestaran des de les instal·lacions de l'empresa adjudicatària, essent obligació d'aquesta l'aportació de les eines necessàries per a la prestació dels serveis de forma remota i assumint els costos de tots els mitjans necessaris per aquesta modalitat de prestació. Durant l'horari de prestació del servei l'empresa adjudicatària i en especial l'equip de treball adscrit a l'execució del contracte, haurà d'estar accessible per via

telefònica i per videoconferència, a través de Microsoft Teams, així com disposar de les eines necessàries per assistir a reunions de forma remota.

En les ocasions que es requereixi, es podrà demanar al personal adscrit als serveis i l'equip de treball del projecte el desplaçament a les oficines de l'IMI o altres dependències, incloses les de l'Ajuntament de Barcelona, per a la prestació d'alguna part del servei en forma temporal o continuada, essent obligació de l'adjudicatari l'aportació de les eines i els mitjans que siguin necessaris per a la prestació d'aquest.

En cas que la prestació del servei es realitzi des de les oficines de l'IMI el prestador estarà obligat a utilitzar els seus propis equips informàtics d'usuari: PC, ordinador portàtil i/o qualsevol altre dispositiu d'informàtica mòbil que consideri necessari. En cap cas l'IMI proveirà dels dispositius informàtics ni telefònics al proveïdor i els desplaçaments necessaris seran a càrrec de l'empresa adjudicatària.

La instal·lació i configuració de l'estàndard corporatiu municipal serà a càrrec de l'adjudicatari sota la supervisió dels equips especialitzats de l'IMI. L'empresa haurà de proveir de línies de comunicació, equips i programari adequat per a la connexió a la infraestructura de l'IMI complint amb la normativa establerta per l'IMI.

9.4 LLENGUA

Obligatòriament l'adjudicatari elaborarà en català la documentació de gestió i documentació tècnica requerida i lliurada durant l'execució del contracte.

L'equip de treball ha de comprendre el català.

9.5 HORARIS

L'horari general de prestació dels serveis és el següent:

- Horari laboral de l'IMI 10 x 5 (de dilluns a divendres de 8:00 h a 18:00 h)

En tot cas, aquest horari serà ampliat en els supòsits particulars que es detallin al llarg del plec, especialment en els apartats 4 i 8.

L'horari preferent per reunions del projecte o de seguiment del servei és el següent:

- Dilluns a divendres entre 9.30 i 14h

El calendari laboral serà el de la ciutat de Barcelona.

9.6 PERÍODE DE GARANTIA DEL CONTRACTE

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

9.7 CLÀUSULA DE GESTIÓ DE SERVEIS TIC

Tota l'activitat dels serveis descrits en aquest plec de prescripcions tècniques es desenvoluparan d'acord amb el model de gestió de serveis TIC de l'IMI, que amb les seves especificitats, està basat en les pràctiques d'ITIL.

Els processos del model de gestió de serveis TIC de l'IMI relacionats amb l'activitat dels serveis objecte d'aquest contracte són els següents:

- Procés de Gestió de Peticions
- Procés de Gestió d'Incidències
- Procés de Gestió de Problemes
- Procés de Gestió d'Esdeveniments
- Procés de Gestió de Canvis
- Procés de Gestió de la Configuració i Inventari
- Procés de Gestió de Versions i Desplegaments
- Procés de Gestió de la Capacitat i Disponibilitat

El detall d'aquests processos es descriuen a l'Annex I: Gestió de Serveis TIC. L'adjudicatari haurà de participar en els diferents processos d'acord amb les responsabilitats que es detallen per a cada procés.

D'altra banda, l'execució dels serveis objecte d'aquest contracte es poden veure afectats per diferents situacions de crisi. L'IMI disposa d'un procediment d'actuació davant els diferents estats d'emergència que es puguin presentar en l'àrea d'operacions.

Es considera crisi quan un incident posa en perill la continuïtat del servei o deriva amb conseqüències importants pel servei/s i l'usuari. Es pot dir que s'entra en crisi en el moment que es genera una discontinuïtat important en el servei, depenent del temps i de l'afectació. En aquest sentit, es deriven diferents nivells o estats d'emergència.

Existeixen 4 nivells diferents d'emergència. Els dos primers (Nivell 0 i nivell 1) formen part de l'operativa habitual d'operacions, cada dia es registren i es gestionen talls de serveis que operen amb aquest nivell de crisi sense que derivin en la seva majoria amb grans conseqüències. El segon bloc format per els nivells 2 i 3 és on podem dir que comença la crisi pròpiament i requereix d'actuacions i decisions que poden estar fora de circuits prèviament establerts.
Segons el nivell de d'emergència, el proveïdor del servei afectat haurà de participar assumint un determinat rol (comunicador/informador o coordinador), amb l'objectiu de deslliurar d'aquesta funció als equips tècnics i els coordinadors d'emergència per a què es concentrin en la resolució. Haurà d'assumir determinades funcions com informar sobre els serveis afectats, presentar informes, comunicar una previsió de resolució, etc.

Els detalls del procediment d'emergència es descriu a l'Annex II: Protocol d'Emergències.

10 CLÀUSULES GENERALS DE SEGURETAT

10.1 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 l'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.

10.2 CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT (ENS)

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).

L'adjudicatari es compromet 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. Donada la naturalesa del contracte, l'adjudicatari haurà de donar compliment als requeriments de nivell **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, respecte del nivell especificat, mitjançant alguna de les següents opcions:

- Certificació oficial d'una entitat de certificació acreditada.

- Informe de compliment. L'adjudicatari serà responsable de disposar d'un informe 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.).

10.3 RESPONSABLE DE SEGURETAT

L'adjudicatari nomenarà un Responsable de Seguretat, el qual haurà de vetllar pel compliment dels següents requeriments:

- Actuar d'interlocutor únic per a tots els aspectes de seguretat del contracte.
- Garantir que tots els serveis prestats pel proveïdor a l'Ajuntament es realitzen d'acord al model i requeriments de seguretat establerts per l'IMI i seguint la normativa de seguretat vigent.
- Garantir i liderar dins la seva organització la correcta implantació dels nivells de seguretat i les seves corresponents mesures (tècniques, organitzatives i jurídiques), així com les directrius en matèria de seguretat establertes per l'IMI.
- Assegurar que tot el personal de l'adjudicatari que prestarà serveis a l'Ajuntament, passi per un pla de conscienciació i formació en matèria de seguretat.
- Informar al seu personal qualsevol obligació a què l'empresa estigui sotmesa per contracte, formar al seu personal en les polítiques i instruccions de l'Administració Municipal en cas que els sigui d'aplicació i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Administració Municipal.
- Mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Administració Municipal, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

10.4 DELEGAT DE PROTECCIÓ DE DADES

Si l'empresa adjudicatària ha anomenat un delegat de protecció de dades, procedirà a comunicar les seves dades de contacte a l'Oficina del Delegat de Protecció de Dades de l'Ajuntament perquè es puguin establir els circuits de comunicació establerts en el Reglament General de Protecció de Dades.

En cas de no haver definit aquesta figura, s'haurà de proporcionar el contacte de la persona encarregada del tractament de dades personals.

10.5 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'empara 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.

10.6 PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Les obligacions en matèria de protecció de dades de caràcter personal seran les fixades en el plec de clàusules administratives particulars.

10.7 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.

10.8 CLÀUSULA SOFTWARE I METODOLOGIA DE DESENVOLUPAMENT

L'empresa contractada, disposarà del software necessari i farà servir la metodologia implantada pel Institut Municipal d'Informàtica (IMI) per al desenvolupament dels serveis contractats.

Si l'Administració Municipal ho considera necessari, es podrà instal·lar software en els equips de l'empresa contractada, sempre sota la responsabilitat de l'empresa contractada, amb la finalitat d'obtenir una correcta prestació dels serveis contractats. Les llicències de software necessàries per desenvolupar el servei correran a càrrec de l'adjudicatari.

L'Administració Municipal continuarà essent la propietària o, en el seu cas, titular dels drets de propietat intel·lectual que el corresponen sobre el software i bases de dades instal·lat en les

màquines de l'empresa contractada, sense que la corresponent llicència d'ús suposi transferència o cessió, total o parcial de la titularitat, ni autorització per la seva utilització amb una finalitat diferent a la definida en el contracte de prestació de serveis.

L'empresa contractada donarà a conèixer a tot el personal adscrit a la prestació dels serveis, el contingut d'aquesta clàusula respecte al software, sistemes operatius i bases de dades cedides per l'Administració Municipal, la seva obligació respecte a:

- No reproduir-los.
- No transmetre'ls a un altre sistema.
- No modificar, adaptar, cedir, ni realitzar qualsevol altre activitat sobre el software cedit, sense l'autorització de l'Administració Municipal.
- No divulgar, publicar, ni posar a disposició d'altres persones diferents a les autoritzades.
- Fer ús única i exclusivament per les tasques encomanades, incloses en els serveis contractats.

La utilització de la metodologia a utilitzar per al desenvolupament i que està inclosa en el punt 4.3 del present plec.

10.9 AUDITORIA

L'IMI auditarà que l'adjudicatari vetlli per la seguretat del seu servei. Es contemplen dos tipus d'auditories:

- Auditoria de seguretat periòdica/planificada: l'IMI podrà realitzar auditories de seguretat planificades per verificar el compliment dels requeriments de seguretat, de l'oferta de l'adjudicatari.
- Auditoria sobrevinguda: addicionalment l'IMI podrà efectuar més auditories que les planificades respecte el servei que s'està prestant.

En tots aquells casos en què l'IMI decideixi la realització d'una auditoria des de les instal·lacions de l'adjudicatari, aquest haurà de garantir a l'IMI l'accés necessari, incondicional i irrevocable als documents existents que estiguin relacionats amb l'abast de l'auditoria.

L'adjudicatari proporcionarà l'assistència i la informació que requereixin les auditories, sense càrrec addicional per l'IMI.

La realització de l'auditoria en cap moment eximirà l'adjudicatari del compliment dels compromisos derivats de la prestació dels serveis.

A la finalització de l'auditoria, es revisaran els resultats i s'elaborarà un pla d'acció per corregir les possibles desviacions i/o observacions detectades. El conjunt del resultat serà signat per ambdues parts.

L'adjudicatari, d'acord amb el calendari establert al pla d'acció, es compromet a portar a terme les activitats establertes en el pla d'acció. L'IMI podrà verificar que el pla d'acció s'ha implementat correctament.

10.10 GESTIÓ D'INCIDENTS

L'adjudicatari informarà a la Direcció de Serveis de Seguretat de la Informació de l'IMI de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert per l'IMI.

L'adjudicatari col·laborarà amb l'IMI-Seguretat en la resolució de qualsevol incident produït en el seu entorn, tot proporcionant totes les evidències requerides.

10.11 ACCÉS A LA INFORMACIÓ

Si l'accés a les dades es fa als locals de l'Ajuntament de Barcelona, o si es fa de forma remota exclusivament a suports o sistemes d'informació de l'Ajuntament, l'adjudicatari té prohibit incorporar les dades a d'altres sistemes o suports sense autorització expressa i haurà de complir amb les mesures de seguretat establertes per l'IMI.

10.12 DIMENSIONAMENT I GESTIÓ DE CAPACITATS

El proveïdor disposarà del personal necessari amb les qualificacions professionals adients, per a la prestació del servei de forma adequada

10.13 ANÀLISISI FORENSES

L'execució d'anàlisis forenses és responsabilitat exclusiva de la Direcció de Seguretat de la Informació de l'IMI. L'adjudicatari haurà de col·laborar proporcionant la informació requerida i el coneixements de les plataformes i tecnològics que facin falta. Les peticions de col·laboració es realitzaran a través dels procediments que s'acordin entre la Direcció de Seguretat de la Informació de l'IMI i l'adjudicatari.

10.14 CONTROL D'ACCÉS

10.14.1 Accés local

L'adjudicatari haurà de protegir les estacions de treball i es compromet a complir les següents condicions:

- La informació revelada a qui intenta accedir ha de ser la mínima imprescindible. Els diàlegs d'accés proporcionaran únicament la informació indispensable.
- El nombre d'intents permesos serà limitat, bloquejant l'oportunitat d'accés una vegada efectuats un cert nombre de fallades consecutives.
- Es registraran els accessos amb èxit, i els fallits.
- El sistema informarà a l'usuari de les seves obligacions immediatament després d'obtenir l'accés.

10.14.2 Accés remot

L'adjudicatari disposarà dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Ajuntament, sent els costos de connexió a càrrec de l'empresa adjudicatària.

La connexió remota als sistemes de l'Ajuntament es realitzarà seguint els protocols establerts per l'IMI per als sistemes de l'Ajuntament.

10.14.3 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.

10.15 GESTIÓ DEL PERSONAL

10.15.1 Deures i obligacions del personal

El Cap de Projecte de l'empresa adjudicatària durà a terme de forma correcta la gestió del personal i els aspectes relacionats amb la seguretat de la informació.

L'empresa adjudicatària està obligada a implantar i donar a conèixer al seu personal els mecanismes i controls necessaris per a garantir l'accessibilitat, la confidencialitat integritat i la disponibilitat de la informació de l'Ajuntament, i de donar-los a conèixer al seu personal.

El Cap de Projecte de l'empresa adjudicatària, abans de l'inici de la prestació del servei objecte del contracte, haurà de notificar al seu personal qualsevol obligació a la que l'empresa estigui sotmesa per contracte i formar al seu personal en la política i instruccions de l'Ajuntament que els sigui d'aplicació.

El Cap de Projecte haurà d'informar a tothom que presti serveis dins del marc del contracte, dels deures i responsabilitats del seu lloc de treball en matèria de seguretat de la informació i protecció de dades de caràcter personal, especificant les mesures disciplinàries al fet que pertoqui i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Ajuntament.

El Cap de Projecte de l'empresa adjudicatària haurà de mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Ajuntament, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

El document d'acceptació de les obligacions signat per les persones adscrites a l'execució d'aquest contracte serà entregat al Cap de Projecte de l'Ajuntament, abans de ser donats els

permisos per accedir als Sistemes d'Informació de l'Ajuntament o bé abans de ser facilitada la informació per al correcte compliment del servei contractat, i restarà en poder de l'empresa adjudicatària que haurà de presentar-los quan siguin requerits per l'Ajuntament.

Es contemplarà el deure de confidencialitat respecte de les dades a les que tingui accés, tant durant el període de duració del contracte, com posteriorment a la seva terminació.

L'empresa adjudicatària haurà de mantenir disponible en tot moment la informació o treballs resultants de l'objecte del contracte, amb la finalitat de comprovar el compliment de les mesures i controls previstos en aquest apartat.

10.15.2 Formació i conscienciació

L'adjudicatari realitzarà les accions necessàries per conscienciar regularment al personal sobre el seu paper i responsabilitat respecte a la seguretat dels sistemes. Es recordarà regularment:

- Instrucció sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part del personal al servei de l'Ajuntament de Barcelona.
- Normativa de seguretat relativa al bon ús dels sistemes.
- Normativa d'identificació i comunicació d'incidents, activitats o comportaments sospitosos que hagin de ser reportats per al seu tractament per personal especialitzat.

L'adjudicatari haurà de formar regularment al personal en aquelles matèries que requereixin per a l'acompliment de les seves funcions, en particular en relació a configuració de sistemes, detecció i reacció a incidents, i gestió de la informació i dades personals en qualsevol tipus de suport.

L'Ajuntament podrà demanar evidències de les diferents accions de formació i conscienciació que l'adjudicatari ha realitzat sobre el personal assignat a l'execució del contracte.

10.16 PROTECCIÓ DEL LLOC DE TREBALL

10.16.1 Lloc de treball buit

L'adjudicatari haurà d'establir una política de "taules netes" respecte a la documentació de l'Ajuntament. Únicament es podrà disposar del material requerit per a l'activitat que s'està realitzant a cada moment.

10.16.2 Protecció d'equips

L'adjudicatari es compromet a que els equips que surtin, o puguin sortir de l'empresa adjudicatària, estaran protegits adequadament contra accessos no autoritzats en cas de pèrdua o robatori.

Sense perjudici de les mesures generals que els afectin, es requereix a l'adjudicatari que porti un inventari d'equips juntament amb una identificació de la persona responsable del mateix i un control regular que està positivament sota el seu control. Els usuaris hauran de disposar d'un canal de comunicació per informar al servei de gestió d'incidents de pèrdues o robatoris, que hauran de ser comunicades a l'IMI.

S'evitarà, en la mesura del possible, que l'equip contingui claus d'accés remot a l'organització. Es consideraran claus d'accés remot aquelles que habilitin un accés a altres equips de l'organització, o unes altres de naturalesa anàloga.

Addicionalment, els equips hauran de disposar:

- Solució antivirus actualitzada a la última versió i configurada per a que realitzi anàlisis regulars de l'equip.
- Política d'actualització que instal·li els últims pegats de seguretat en un temps raonable, prioritzant aquelles actualitzacions crítiques.
- *Firewall* habilitat restringint el trànsit entrant a l'equip al mínim necessari.

10.17 CLÀUSULA DE COMUNICACIONS EXTERNES

L'adjudicatari disposarà dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Administració Municipal, sent els costos de connexió a càrrec de l'empresa contractada.

La connexió és realitzarà seguint els protocols de seguretat per a les comunicacions externes establerts per l'Administració Municipal.

L'adjudicatari serà el responsable de custodiar correctament els certificats digitals lliurats per la interconnexió segura de xarxes i de demanar la seva revocació una vegada finalitzada la prestació del servei. Així mateix, serà responsable subsidiària de l'ús del certificats personals individuals lliurats als seus empleats pel desenvolupament del producte o servei.

10.18 PROTECCIÓ DELS SUPORTS INFORMÀTICS

10.18.1 Etiquetat

L'adjudicatari es compromet a etiquetar els suports d'informació de manera que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de major qualificació. Els usuaris han d'estar capacitats per entendre el significat de les etiquetes, bé mitjançant simple inspecció, bé mitjançant el recurs a un repositori que ho expliqui.

10.18.2 Transport

L'adjudicatari garantirà que els dispositius romanen sota control i que satisfan els requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre. L'adjudicatari garantirà que es segueix el procediment de transport, de manera que s'haurà de disposar d'un registre de sortida que identifiqui al transportista que rep el suport per al seu trasllat i d'un registre d'entrada que identifiqui al transportista que el lliura, conjuntament amb un procediment rutinari que quadri les sortides amb les arribades i elevi les alarmes pertinents quan es detecti algun incident.

10.18.3 Esborrat i destrucció

L'adjudicatari haurà de seguir els estàndards i normes de l'IMI respecte a l'esborrat i destrucció de suports d'informació. S'aplicarà a tot tipus d'equips susceptibles d'emmagatzemar informació, incloent mitjans electrònics i no electrònics. Els suports que hagin de ser reutilitzats per a una altra informació o alliberats a una altra organització hauran de ser objecte d'un esborrat segur del seu contingut.

Periòdicament i segons les necessitats de recurrència d'aquestes activitats, s'haurà d'informar i lliurar al responsable del contracte el certificat de destrucció corresponent, on quedarà especificat com a mínim, el identificador dels actius, el mètode d'esborrat i/o destrucció emprat, la data de l'activitat i el destí dels actius.

10.19 PROTECCIÓ DE LA INFORMACIÓ

10.19.1 Neteja de documents

L'adjudicatari disposarà d'un procediment de neteja de documents, el qual retirarà d'aquests tota la informació addicional continguda en camps ocults, metadades, comentaris o revisions anteriors, excepte quan aquesta informació sigui pertinent per al receptor del document.

Aquesta mesura serà especialment rellevant quan el document es difongui àmpliament, com quan s'ofereix al públic en un servidor web o un altre tipus de repositori d'informació.

10.19.2 Protecció del correu electrònic

En el cas de que l'adjudicatari faci ús del seu correu electrònic corporatiu per gestionar informació de l'Ajuntament, l'haurà protegir enfront d'amenaces que li són pròpies:

- La informació distribuïda per mitjà de correu electrònic, es protegirà, tant en el cos dels missatges, com en els annexos.
- Es protegirà la informació d'encaminament de missatges i establiment de connexions.
- No es permetrà la redirecció a dominis de correus públics fora del correu corporatiu de l'adjudicatari.
- Es protegirà a l'organització enfront de problemes que es materialitzen per mitjà del correu electrònic, en concret:
    - Correu no sol·licitat (*spam*)
    - Programes nocius, constituïts per virus, cucs, troians, espies, o uns altres de naturalesa anàloga
    - Codi mòbil de tipus *applet*.

L'adjudicatari establirà polítiques d'ús del correu electrònic que inclourà com a mínim:

- Limitacions a l'ús com a suport de comunicacions privades.
- Realitzar activitats de conscienciació i formació relatives a l'ús del correu electrònic per al seu personal, per exemple per detectar casos de *malware* o *phishing*.

El responsable del contracte de l'Ajuntament avaluarà si el contracte ha de gestionar informació sensible, especialment protegida en relació a la protecció de dades personals, confidencial de l'Ajuntament o de les tecnologies municipals (adreces IP, usuaris, credencials,...)

En cas afirmatiu, l'Ajuntament facilitarà a l'empresa adjudicatària un correu electrònic de l'Ajuntament (@ext.bcn.cat) el qual es convertirà en la via de comunicació entre l'empresa adjudicatària i l'Ajuntament.

Aquesta mesura vol evitar que les empreses externes retinguin informació confidencial de l'Ajuntament en servidors de correu aliens a l'entorn municipal, durant i sobretot, un cop finalitzat el contracte.

10.20 PROTECCIÓ DE LES INSTAL·LACIONS

Les instal·lacions de l'adjudicatari hauran de disposar de certes condicions de seguretat física:

- En cas de emmagatzemar informació de l'Ajuntament de Barcelona, disposar de les mesures de seguretat pertinents per evitar els accessos físics als repositoris d'informació, segons la sensibilitat de dita informació.

- Garantir que la informació de l'Ajuntament de Barcelona no pugui ser visible i/o audible des de l'exterior de les instal·lacions

10.21 GESTIÓ D'EXCEPCIONS

Qualsevol excepció als anteriors apartats no recollida en el present document en el moment de la contractació o que ocorri en el transcurs del servei, haurà de ser comunicada per mitjà dels canals oficials a la Direcció de Seguretat de la Informació de l'IMI per al seu corresponent tractament i valoració. S'haurà de presentar de forma clara i concisa l'objecte de l'excepció així com la modificació desitjada pel sol·licitant amb la seva deguda justificació

10.22 GESTIÓ D'IDENTITATS I 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.

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.

10.23 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.

10.24 DESENVOLUPAMENT SEGUR

L'adjudicatari es compromet a adequar les seves polítiques i procediments de desenvolupament de programari de tal forma que el seu cicle de desenvolupament de software garanteixi la seguretat en els productes desenvolupats.

Els següents elements seran part integral del disseny del sistema:

- Els mecanismes d'identificació i autenticació.
- Els mecanismes de protecció de la informació.
- La generació i tractament de pistes d'auditoria.

El prestador està obligat a realitzar una revisió del codi font per a tots els desenvolupaments que siguin lliurats, ja sigui per al desenvolupament d'un aplicatiu, manteniment del mateix o desenvolupaments correctius, amb l'objecte de verificar si existeix alguna vulnerabilitat o amenaça en el desenvolupament realitzat, i si s'escau, procedir a la reparació de la mateixa.

L'IMI en qualsevol moment podrà realitzar una revisió del codi font. Si es detectés algun tipus de vulnerabilitat es comunicarà a l'adjudicatari per tal que procedeixi a arreglar les mancances detectades.

Per a millorar el procés de desenvolupament segur d'aplicacions, l'adjudicatari haurà de realitzar accions addicionals per a garantir la qualitat i seguretat del producte final. Aquestes accions són:

- Emprar una eina d'anàlisi de codi estàtic (SAST) per trobar vulnerabilitats de seguretat al codi font i garantir els bons estàndards de codificació. La periodicitat dels anàlisis hauran de ser acordats conjuntament amb el responsable del contracte. El software emprat al IMI correspon a l'eina SonarQube amb la modalitat OWASP, sent aquesta la tecnologia desitjable a emprar per l'adjudicatari.
- Per al cas particular d'aplicacions conteneritzades, l'adjudicatari haurà de fer ús d'un software d'anàlisis d'imatges Docker. La tecnologia emprada a l'IMI i la preferent d'ús per part de l'adjudicatari és Coreos Clair.

10.25 ACCEPTACIÓ I POSTA EN SERVEI

Abans de passar a producció l'adjudicatari comprovarà el correcte funcionament de l'aplicació es comprovarà que:

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

10.26 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 traves 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'autentificació de llocs web d'acord amb les polítiques establertes per Departament de Seguretat de l'IMI.

10.27 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.

10.28 XIFRATGE

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 IMI-Seguretat. La Direcció de Serveis de Seguretat de la Informació de l'IMI ha d'assegurar la disponibilitat de la informació als propietaris d'aquesta dins de l'Ajuntament i 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.

10.29 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 valides per IMI-Seguretat 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 pel Departament de Seguretat de l'IMI. En tot cas s'ha de complir la política de signatura electrònica de l'ajuntament de Barcelona.

10.30 CERTIFICATS

La Direcció de Serveis de Seguretat de la Informació serà la 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 de l'IMI 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.

10.31 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 dissenyar les traces necessàries en base al Document del 'Pla de Seguretat i Traces' que posarà a disposició l'IMI a l'inici del contracte.

Un cop dissenyades les traces s'haurà d'incorporar aquest disseny 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.

10.32 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.

10.33 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.

10.34 MANTENIENT

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.

10.35 ANTIMLWARE

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.

10.36 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.

10.37 EXPLOTACIÓ

10.37.1 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.

10.37.2 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

10.37.3 Protecció de claus criptogràfiques

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

Sra. Ana Maria Roca Fontanals

Cap del Departament de Serveis Llocs de Treball

Sra. Mònica Estopà Ramírez

Direcció de Serveis al Lloc de Treball de l'IMI

11 INFORMACIÓ ADDICIONAL I ACLARIMENTS

Si és de l'interès dels licitadors sol·licitar informació addicional per a la presentació de l'oferta, l'IMI posarà a disposició les següents adreces de correu on aquestes podran realitzar les seves consultes:

jcalvoa@bcn.cat ahomsm@bcn.cat jgarrudo@bcn.cat

En l'assumpte del correu cal indicar:

Contracte: S0088 - Contracte implantació nou Gestor d'Identitats i provisió serveis gestió i govern d'identitats i accessos

S'atendran les sol·licituds d'informació rebudes fins a 3 dies hàbils abans de la data límit de presentació d'ofertes. Les respostes es publicaran degudament a la plataforma de contractació pública.

Per tal que les empreses licitadores interessades a presentar oferta puguin aclarir els dubtes que els sorgeixin, l'IMI posa a la seva disposició les bústies de correu abans indicades per qüestions tècniques i la de imi_gestio_contractacio@bcn.cat per consultes de caràcter administratiu.

Així mateix, s'indica que, inicialment, no es convocarà sessió informativa per a aquesta licitació. Malgrat això, si alguna de les empreses licitadores estigués interessada a realitzar-la, pot fer-ne la petició a través del correu imi_gestio_contractacio@bcn.cat.

Les consultes rebudes dins dels 3 dies hàbils anteriors a la data de finalització d'entrega de les proposicions seran solucionades i publicades al perfil del contractant de l'IMI:

https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/cap.pscp?reqCode=viewDetail&idCap=15990903

12 ANNEX. I GESTIÓ DE SERVEIS TIC

<Es troba en document separat>

13 ANNEX II. PROTOCOL D'EMERGÈNCIES

<Es troba en document separat>