



**Ajuntament
de Barcelona**

Institut Municipal d'Informàtica
Direcció d'Operacions i Sistemes

Plec de prescripcions tècniques per a construcció de la solució CA AUTOMIC AWA (Automic Workload Automation) per canvi de versió, amb mesures de contractació pública sostenible.



ÍNDEX

1. INTRODUCCIÓ	4
2. OBJECTE	4
3. ABAST	4
4. ORGANITZACIÓ	6
5. CONDICIONS D'EXECUCIÓ	6
5.1. LLOC DE PRESTACIÓ DEL CONTRACTE	6
5.2. GARANTIA	6
6. OFERTA ECONÒMICA	7
6.1. FACTURACIÓ	7
7. PROPOSTA TÈCNICA	7
8. CLAUSULES GENERALS DE SEGURETAT	7
8.1. SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES	7
8.2. RESPONSABLE DE SEGURETAT	8
8.3. CLÀUSULA PER ACCESSOS POTENCIALS	9
8.4. CONFIDENCIALITAT	9
8.5. CLÀUSULA PROGRAMARI I METODOLOGIA DE DESENVOLUPAMENT	10
8.6. AUDITORIA	10
8.7. GESTIÓ D'INCIDENTS	11
8.8. ANÀLISIS FORENSES	11
8.9. CONFIDENCIALITAT	12
8.10. DIMENSIONAMENT/GESTIÓ DE CAPACITATS	12
8.11. ACCÉS A LA INFORMACIÓ	12
8.12. CONTROL D'ACCÉS	12
8.12.1. Accés local	12
8.13. GESTIÓ DEL PERSONAL	13
8.13.1. Deures i obligacions del personal	13
8.13.2. Formació i conscienciació	13
8.14. PROTECCIÓ DEL LLOC DE TREBALL	14
8.14.1. Lloc de treball buit	14
8.14.2. Bloqueig del lloc de treball	14
8.14.3. Protecció d'equips	14
8.15. PROTECCIÓ DE LA INFORMACIÓ	15
8.15.1. Neteja de documents	15



8.15.2.	Protecció del correu electrònic	15
8.16.	GESTIÓ D'IDENTITATS, AUTENTICACIÓ D'USUARIS _____	16
8.17.	AUTORITZACIÓ DELS USUARIS ALS SISTEMES _____	16
8.18.	PROTECCIÓ DE LES APLICACIONS I SERVEIS WEB _____	18
8.19.	ACCEPTACIÓ I POSTA EN SERVEI _____	18
8.20.	EXPORTACIÓ DE LA BASE DE DADES _____	18
8.21.	DADES DE PROVES _____	19
8.22.	PLA DE TRACES _____	19
8.1.	GESTIÓ D'EXCEPCIONS _____	19
8.2.	ANNEX 1: INFORMACIÓ ADDICIONAL / ACLARIMENTS _____	21



1. INTRODUCCIÓ

L'Ajuntament de Barcelona requereix en diversos dels seus departaments de l'execució de processos Batch.

Per donar cobertura a aquest fet, l'Institut Municipal d'informàtica (en endavant IMI) te implantat als seus sistemes un planificador Batch amb tots els processos Batch dels diferents departaments de l'Ajuntament de Barcelona.

El planificador de processos Batch implantat a l'IMI es CA Automic en la seva versió 12.3. Aquesta versió es troba fora de suport per part del fabricant des del 30 de Juny del 2023, per tant ens veiem en la necessitat de construir una solució més actual i que gaudeixi de suport per part del fabricant.

Considerem aquest planificador Batch idoni per a les nostres necessitats municipals, al tractar-se de productes molt estesos al mercat i consolidats amb molts anys d'experiència pel que fa a la seva implantació a l'Ajuntament de Barcelona.

Aquest contracte dóna servei de continuïtat a sistemes d'informació i necessitats de diversos departaments de tot l'Ajuntament de Barcelona que són necessaris per a la gestió dels serveis que presta a la ciutadania. El correcte funcionament d'aquests sistemes són del tot necessaris per tal que es proporcioni un servei eficient i de qualitat als ciutadans per part del personal que els fa servir, motius pels quals fa que esdevingui un servei d'interès públic.

2. OBJECTE

L'objecte d'aquest contracte és la construcció de la solució més actual del planificador batch CA Automic, que actualment tenim a la versió 12.3, i de tots els seus components que formen el sistema, amb mesures de contractació pública sostenible.

3. ABAST

En concret es demana la realització de les següents tasques per a realitzar l'actualització del producte:

Tasques implicades en el canvi de versió :

- Assegurar l'actual instal·lació d'Automic
- Creació del pla de construcció
- Exportació de la Base de Dades
- Actualització d'Automic Automation Engine
- Importació de la Base de Dades
- Actualització d'Automic Dialog Clients (actualment ECC)
- Actualització dels Automic Agents (95 Agents aprox.)



- Test del nou entorn d'Automic

Millors pràctiques per la construcció del nou planificador CA Automic AWA

1. Preparació :

- Comparar notes v.12.3 vs ultima versió
- Comprovar requeriments de software, hardware i base de dades
- Anotar canvis en la estructura de base de dades [UC_UPD.TXT]
- Comprovar i actualitzar qualsevol indexació creada [UC_DDL.SQL]
- Reorganitzar Base de Dades d'Automic utilitzant la menor quantitat possible de paràmetres.
- Habilitar accés remot amb usuari administrador.

2. Test del procés d'actualització :

- Crear còpia de la Base de dades actual a l'entorn de test.
(Es realitzarà el procés d'actualització de la base de dades amb una còpia de l'entorn de producció. S'anotaran els temps de processament com a referència per planificar el procediment d'actualització productiu. El procés inclourà reports generats en el sistema, i només en cas que el temps de processament estigui fora d'un rang normal en funció del volum, es contemplarà la possibilitat d'ometre la inclusió dels reports en el procés d'actualització.)
- Buidar taules MQ* i E*.
- Instal·lar les utilitats Automation Server, User Interface (ECC) i Agents
- Executar la utilitat DBLoad per analitzar la Base de Dades.
- Iniciar Automic Automation Engine en mode "COLD"

3. Actuacions en el sistema Test

- Testejar la User Interface, la ajuda online, els Call API, etc..
- Comprovar l'execució de diferents objectes
- Test de noves funcionalitats de la nova versió
- Bateria de proves per verificar la inexistència de errors en el procés de canvi de versió. Els objectes que es desitgen provar seran indicats per IMI per validar el procés d'integració.
- Configuració de noves funcionalitats de la versió.

4. Comprovar la construcció en el sistema de Test

- Adquirir confiança sobre la nova versió en el sistema de test
- Executar i monitoritzar les tasques de producció
- Integrar noves funcionalitats
- Un cop validat l'entorn de test, planificar el procés d'actualització per l'entorn productiu.
- Delta nova versió – Revisió dels principals canvis funcionals
- Elaboració d'un pla de marxa enrere per producció.



- Formació a usuaris sobre els principals canvis funcionals amb la nova versió

5. Construcció del sistema productiu :

- Planificar i realitzar l'actualització en el sistema productiu.
(Es realitza el procés d'actualització de la base de dades de producció. El procés d'arrancada de la nova versió es programarà en funció de les necessitats i requeriments del servei de l'IMI, tenint en compte que s'haurà de parar el sistema productiu unes hores.)
- Comprovacions de funcionalitat, us i rendiment
- Nova versió de CA Automic en producció.

4. ORGANITZACIÓ

L'IMI disposa d'un equip encarregat i especialitzat en el planificador batch. Aquest equip serà l'interlocutor per part de l'IMI i tindrà la responsabilitat de validar el correcte lliurament dels serveis demanats a l'adjudicatari.

L'adjudicatari entregarà per correu un Resum Executiu a l'equip encarregat en el planificador batch en IMI a l'inici del contracte. Aquest Resum Executiu haurà d'incloure la seva proposta de tasques per realitzar la migració així com el temps necessari per cadascuna d'elles; així mateix inclourà el detall de la seva proposta d'organització per tal d'assegurar de forma òptima els serveis indicats a l'apartat 3 d'aquest mateix document.

Per altre banda, i com a mínim oferirà un contacte tècnic expert en CA Automic i un contacte administratiu que es responsabilitzarà dels aspectes comercials i administratius durant l'execució del contracte.

5. CONDICIONS D'EXECUCIÓ

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

5.1. LLOC DE PRESTACIÓ DEL CONTRACTE

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

5.2. GARANTIA

Aquest contracte tindrà 6 mesos de garantia posteriors al pas a producció de la realització de l'actualització d'Automic.



6. OFERTA ECONÒMICA

Els licitadors presentaran la seva oferta econòmica (IVA exclòs) a tant alçat d'acord amb el model d'oferta econòmica que s'adjunta al plec de clàusules administratives particulars.

6.1. FACTURACIÓ

L'adjudicatari facturarà la totalitat de l'import una vegada hagi realitzat el servei i aquests estigui productiu al sistema. La factura s'emetrà un cop l'actualització hagi estat validada pels serveis tècnics de l'IMI. També serà necessari per poder emetre aquesta factura s'hagi lliurat tota la documentació del producte així com els manuals d'usuari.

7. PROPOSTA TÈCNICA

Els licitadors presentaran la seva proposta d'acord amb els criteris d'adjudicació assenyalats en el plec de clàusules administratives particulars que regeixen aquesta contractació.

Els licitadors l'hauran de presentar a través de la plataforma electrònica, conforme s'estableix al plec de clàusules administratives que regeix la present licitació. A l'oferta en suport electrònic tots els arxius hauran d'estar en format **Open Document (odt o odp) o pdf obligatori, en format no protegit, amb fonts incrustades i que accepti cerques, seleccions i copiat del text.**

El licitador pot adjuntar tota la informació complementària que consideri d'interès, tot i això haurà de presentar uns continguts mínims i estar obligatòriament estructurada de la forma següent:

Es presentarà un sobre electrònic denominat **AC, que haurà de contenir l'oferta econòmica d'acord amb el model que s'annexa al plec de clàusules administratives particulars que regeixen per aquesta contractació.**

A l'interior del sobre s'haurà d'incorporar una relació, en arxius independent, dels documents que hi conté ordenats numèricament.

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

8. CLAUSULES GENERALS DE SEGURETAT

8.1. SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES

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 dependent 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 Garantir dels Drets Digitals, així com de la resta de normativa aplicable.

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 3/2010 de 8 de gener pel qual es regula l'Esquema Nacional de Seguretat en l'Àmbit de l'Administració Electrònica.

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

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

8.2. 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 el projecte es realitza 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.

8.3. CLÀUSULA PER ACCESSOS POTENCIALS

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

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

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

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

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

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

8.4. 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.

8.5. CLÀUSULA PROGRAMARI I METODOLOGIA DE DESENVOLUPAMENT

L'empresa contractada, disposarà del programari 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 programari 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 programari 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 programari, 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 programari 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 7 del present plec.

8.6. AUDITORIA

L'IMI es reserva el dret de vetllar per la qualitat del servei prestat per l'adjudicatari. 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 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.

8.7. GESTIÓ D'INCIDENTS

L'adjudicatari informarà a l'IMI-Seguretat 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. Incidents susceptibles de ser reportats poden ser, entre d'altres, la pèrdua de dispositius amb informació de l'Ajuntament o la infecció d'actius amb connectats a la xarxa corporativa.

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

8.8. ANÀLISIS FORENSES

L'execució d'anàlisis forenses és responsabilitat exclusiva de l'IMI-Seguretat. 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 IMI-Seguretat i el Proveïdor.



8.9. CONFIDENCIALITAT

L'empresa contractada 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'Administració Municipal.

L'empresa contractada 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 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'empresa contractada es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per l'Administració Municipal, així com qualsevol altre producte obtingut com a resultat del present contracte.

8.10. DIMENSIONAMENT/GESTIÓ DE CAPACITATS

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

8.11. ACCÉS A LA INFORMACIÓ

Tant 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 altres sistemes o suports sense autorització expressa i haurà de complir amb les mesures de seguretat establertes per l'IMI.

8.12. CONTROL D'ACCÉS

8.12.1. Accés local

L'adjudicatari haurà de protegir les estacions de treball amb les quals durà a terme el projecte 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.



8.13. GESTIÓ DEL PERSONAL

8.13.1. 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.

8.13.2. 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.

8.14. PROTECCIÓ DEL LLOC DE TREBALL

8.14.1. Lloc de treball buit

L'adjudicatari haurà d'adoptar la política de l'Ajuntament "taules netes" respecte a la documentació que pugui tractar en el desenvolupament del projecte. Únicament es podrà disposar del material requerit per a l'activitat que s'està realitzant a cada moment.

El material haurà de quedar guardat en un espai tancat quan no s'estigui utilitzant.

8.14.2. Bloqueig del lloc de treball

L'adjudicatari garantirà que els seus equips es bloquejaren al cap d'un temps prudencial d'inactivitat, requerint una nova autenticació de l'usuari per reprendre l'activitat.

8.14.3. 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.

Adicionalment, 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 tràfic entrant a l'equip al mínim necessari.

8.15. PROTECCIÓ DE LA INFORMACIÓ

8.15.1. 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.

8.15.2. 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'amenaques 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*.

Si l'Ajuntament considera que la informació tractada pel contracte és prou sensible, facilitarà a l'adjudicatari un correu electrònic de l'Ajuntament el qual es convertirà en la via de comunicació entre l'adjudicatari i l'Ajuntament.

8.16. GESTIÓ D'IDENTITATS, AUTENTICACIÓ D'USUARIS

La gestió d'identitats dels usuaris del sistema haurà de complir les polítiques d'usuari, administradors i contrasenyes definides per l'IMI les quals es troben a disposició dels sol·licitants. 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 repositori central per a l'autenticació dels usuaris. La solució d'autenticació corporativa utilitzada per l'IMI és l'Oracle Access Manager (OAM) que proveeix el Single Sign On corporatiu.

La integració amb l'OAM es podrà fer mitjançant les següents opcions:

- Integració mitjançant capçaleres.
- Integració mitjançant l'estàndard SAML 2.0.
- Integració mitjançant l'estàndard OAuth 2.0.

Autenticació externa

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

8.17. AUTORITZACIÓ DELS USUARIS ALS SISTEMES

L'IMI disposa d'un mecanisme d'autorització d'usuari corporatiu basat en el producte Oracle Unified Directory (OUD). L'adjudicatari haurà d'assegurar que les autoritzacions es troben delegades en el repositori central d'autorització (OUD).



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

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. El temps dedicat normalment a integrar un connector estàndard amb una BBDD Oracle és aproximadament 80 hores d'un tècnic.

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 per IMI-Seguretat.

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 perfils (rols) de seguretat. Entenent com a perfil o 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.



8.18. 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, aplicant segons apliqui les següents mesures:

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

8.19. ACCEPTACIÓ I POSTA EN SERVEI

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

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

8.20. EXPORTACIÓ DE LA BASE DE DADES

En el moment que es requereixi l'exportació de la Base de Dades, aquest procés haurà de seguir els procediments d'autorització establerts per Seguretat, el qual valorarà les mesures de seguretat necessàries per dur a terme l'operació.



8.21. 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, tal i com es menciona a l'apartat 4. Organització.

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

8.22. PLA DE TRACES

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

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

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

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

8.1. 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



**Ajuntament
de Barcelona**

Institut Municipal d'Informàtica
Direcció d'Operacions i Sistemes

oficials a IMI-Seguretat 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.

Aquest plec de prescripcions tècniques ha estat emès pel Sr. Àngel Romero Esteban, tècnic responsable del contracte, adscrit a la Direcció d'Operacions i sistemes de l'IMI, amb el vistiplau de,

Amparo Rodríguez Rodríguez
Directora d'Operacions i sistemes de l'IMI



ANNEXOS

8.2. ANNEX 1: INFORMACIÓ ADDICIONAL / ACLARIMENTS

Si és de l'interès dels licitadors sol·licitar informació per a la presentació de l'oferta, l'IMI posarà a disposició la següent adreça de correu on els licitadors podran fer les seves consultes: imi_expl_ofbatch@bcn.cat.

En l'assumpte del correu, cal indicar: Actualització CA Atomic

En cas de no obtenir resposta, contactar amb el telèfon 93 291 83 66.

S'atendran les sol·licituds d'informació fins a 3 dies laborables abans de la data límit de presentació d'ofertes.