



Plec de prescripcions tècniques per a la contractació dels serveis d'aprovisionament d'infraestructura, serveis de manteniment i govern, així com manteniment de seguretat de webs LAMP de la Direcció de Comunicació de l'Ajuntament de Barcelona amb mesures de contractació pública sostenible



Índex de continguts

1. INTRODUCCIÓ	13
2. OBJECTE	15
3. ABAST.....	16
3.1. MANTENIMENT CORRECTIU.....	17
3.1.1. <i>Gestió d'incidències.....</i>	<i>18</i>
3.2. MANTENIMENT RECURRENT	19
3.2.1. <i>Canvis normatius.....</i>	<i>21</i>
3.2.2. <i>Actualitzacions tecnològiques.....</i>	<i>21</i>
3.2.3. <i>Qualitat tècnica.....</i>	<i>30</i>
3.2.4. <i>Avaluació de noves necessitats.....</i>	<i>31</i>
3.2.5. <i>Acompanyament i recepció de nous projectes.....</i>	<i>32</i>
3.2.6. <i>Millores funcionals i parametrització</i>	<i>35</i>
3.2.7. <i>Formació.....</i>	<i>35</i>
3.2.8. <i>Sondes de monitorització i consultes preventives.....</i>	<i>37</i>
3.2.9. <i>Transició</i>	<i>38</i>
3.3. DESENVOLUPAMENT D'EVOLUTIUS IDENTIFICATS.....	42
3.4. SERVEIS D'EVOLUTIUS RECURRENTS.....	43
3.4.1. <i>Evolutius motivats per canvis normatius.....</i>	<i>44</i>
3.4.2. <i>Evolutius motivats per actualitzacions tecnològiques.....</i>	<i>45</i>
3.4.3. <i>Evolutius motivats per qualitat tècnica</i>	<i>45</i>
3.4.4. <i>Evolutius motivats per millores funcionals i parametrització</i>	<i>45</i>
3.5. SERVEIS TRANSVERSALS DE MANTENIMENT (STM).....	46
3.5.1. <i>Operació.....</i>	<i>47</i>
3.5.2. <i>Suport.....</i>	<i>61</i>
3.5.3. <i>Gestió del canvi.....</i>	<i>65</i>
3.5.4. <i>Gestió del contracte.....</i>	<i>67</i>
3.5.5. <i>Llicències i productes.....</i>	<i>72</i>
3.6. SERVEI D'APROVISIONAMENT D'INFRAESTRUCTURA.....	73
3.6.1. <i>Infraestructura Webs CMS (PaaS).....</i>	<i>74</i>
3.6.2. <i>Infraestructura Servidors Virtuals Dedicats (IaaS)</i>	<i>74</i>
3.6.3. <i>Programari com a servei (SaaS).....</i>	<i>74</i>
3.6.4. <i>Suport a la infraestructura.....</i>	<i>74</i>
4. CONDICIONS GENERALS DE LA PRESTACIÓ DEL SERVEI.....	75
4.1. LOCALITZACIÓ DE LA PRESTACIÓ DELS SERVEIS	75
4.2. HORARIS DE LA PRESTACIÓ DELS SERVEIS	75
4.2.1. <i>Horari base.....</i>	<i>75</i>
4.2.2. <i>Horaris excepcionals.....</i>	<i>76</i>
4.3. IDIOMA.....	76
4.4. PERÍODE DE GARANTIA	77
4.5. ARQUITECTURES I INFRAESTRUCTURA	78
4.5.1. <i>Entorn cloud públic AWS</i>	<i>78</i>



4.5.2.	Entorn Cloud Privat de l'IMI.....	79
4.5.3.	Estàndards d'integració: API Manager(API Connect).....	80
4.5.4.	Infraestructura necessària per a la prestació del servei.....	83
4.5.5.	Components de software lliure.....	85
4.6.	FACTURACIÓ.....	85
4.6.1.	Servei de manteniment correctiu.....	86
4.6.2.	Servei de manteniment recurrent.....	86
4.6.3.	Servei d'evolutius recurrents.....	87
4.6.4.	Serveis Transversals de Manteniment.....	87
4.6.5.	Servei d'aprovisionament d'infraestructura.....	88
4.6.6.	Transició: Subcontractació del servei de "La Mercè".....	88
5.	MODEL DE PRESTACIÓ DEL SERVEI.....	89
5.1.	RELACIÓ DE ROLS IMI/ADJUDICATARI.....	89
5.1.1.	Perfils IMI.....	90
5.1.2.	Perfils adjudicatari.....	91
5.2.	MODEL DE GOVERN.....	97
5.2.1.	Comitè de Seguiment Operatiu.....	98
5.2.2.	Comitè Tècnic.....	99
5.2.3.	Comitè de Direcció.....	99
6.	EINES DEL SERVEI.....	101
7.	QUALITAT DELS SERVEIS.....	102
7.1.	PLA DE QUALITAT.....	102
7.2.	QUALITAT DEL SERVEI.....	102
7.3.	AUDITORIES.....	103
7.3.1.	Objectiu de les Auditories.....	103
7.3.2.	Procediment d'Auditoria.....	104
7.3.3.	Resultats de l'Auditoria.....	104
7.3.4.	Resultats de la Revisió.....	105
7.4.	QUALITAT DE PROGRAMARI.....	105
8.	ACORDS DE NIVELL DE SERVEI (ANS).....	105
8.1.	ANS DE QUALITAT OPERATIVA DEL SERVEI.....	106
8.1.1.	Servei de manteniment correctiu.....	107
8.1.2.	Serveis de manteniment recurrent.....	108
8.1.3.	Serveis d'evolutius identificats.....	108
8.1.4.	Serveis Evolutius Recurrents.....	108
8.1.5.	Serveis Transversals de Manteniment.....	109
8.1.6.	Aplicació de pegats de sistema.....	111
8.1.7.	Disponibilitat de la infraestructura.....	111
9.	REQUERIMENTS ESPECÍFICS.....	113
9.1.	SER0188 INFRAESTRUCTURES WEB.....	113
9.2.	REQUISITS GENERALS DEL CLOUD PRIVAT DE L'IMI.....	113
9.2.1.	Usabilitat.....	113



9.2.2.	<i>Eficiència.....</i>	114
9.2.3.	<i>Validacions de camps</i>	115
9.2.4.	<i>Logs d'execució dels processos batch.....</i>	115
9.2.5.	<i>Calendaris i valors per defecte.....</i>	115
9.2.6.	<i>Processos massius</i>	115
9.2.7.	<i>Processos en batch i on-line.....</i>	116
9.2.8.	<i>Planificador batch UC4.....</i>	116
9.2.9.	<i>Retrocessió</i>	116
9.2.10.	<i>Geocodificació d'adreces.....</i>	117
9.2.11.	<i>Notificació electrònica.....</i>	117
9.2.12.	<i>Generació de documents</i>	117
9.2.13.	<i>Publicació d'edictes.....</i>	118
9.2.14.	<i>Assignació de rols.....</i>	118
9.2.15.	<i>Llistats, informes i explotació de la informació</i>	119
9.2.16.	<i>Proves de Càrrega</i>	120
9.2.17.	<i>Proves de Regressió.....</i>	120
9.2.18.	<i>Monitorització del servei.....</i>	120
9.3.	REQUISITS D'ARQUITECTURA DEL CLOUD PRIVAT DE L'IMI	120
9.4.	REQUISITS DE SEGURETAT	128
9.4.1.	<i>Seguretat de l'aplicació</i>	128
9.4.2.	<i>Control d'accés</i>	129
9.4.3.	<i>Gestió de les Autoritzacions.....</i>	130
9.4.4.	<i>Registre d'activitats del sistema. Auditabilitat i traçabilitat.....</i>	132
9.4.5.	<i>Pla de traces</i>	132
9.4.6.	<i>Emmascarament de dades de caràcter personal</i>	133
9.4.7.	<i>Canvi organitzatiu.....</i>	133
9.5.	ESTÀNDARDS DE DESENVOLUPAMENT	134
9.5.1.	<i>Per a tecnologia Python</i>	134
9.5.2.	<i>Per a tecnologia Drupal (PHP).....</i>	134
9.6.	METODOLOGIA DE DESENVOLUPAMENT	134
9.6.1.	<i>Qualitat de codi.....</i>	134
9.6.2.	<i>Metodologia de treball a aplicar (Dockers).....</i>	135
10.	PROPOSTA TÈCNICA.....	139
10.1.	CONTINGUT SOBRE ELECTRÒNIC B.....	139
10.2.	CONTINGUT SOBRE ELECTRÒNIC C.....	141
11.	CONDICIONS GENERALS D'EXECUCIÓ	142
11.1.	RESPONSABLE DE SEGURETAT	142
11.2.	DELEGAT DE PROTECCIÓ DE DADES.....	143
11.3.	AUDITORIA	143
11.4.	GESTIÓ D'INCIDENTS DE SEGURETAT	144
11.5.	CONFIDENCIALITAT	145
11.6.	DIMENSIONAMENT/GESTIÓ DE CAPACITATS.....	145
11.7.	ACCÉS A LA INFORMACIÓ.....	145
11.8.	ANÀLISIS FORENSES.....	146



11.9.	CONTROL D'ACCÉS	146
11.9.1.	Accés local	146
11.9.2.	Accés remot.....	146
11.10.	GESTIÓ DEL PERSONAL.....	146
11.10.1.	Deures i obligacions del personal.....	146
11.10.2.	Formació i conscienciació.....	147
11.11.	CLÀUSULA DE COMUNICACIONS EXTERNES.....	148
11.12.	PROTECCIÓ DEL LLOC DE TREBALL	148
11.12.1.	Lloc de treball buit.....	148
11.12.2.	Bloqueig del lloc de treball.....	148
11.12.3.	Protecció d'equips	148
11.12.4.	Medis alternatius.....	149
11.13.	PROTECCIÓ DELS SUPORTS INFORMÀTICS	149
11.13.1.	Etiquetat	149
11.13.2.	Criptografia	149
11.13.3.	Transport.....	150
11.13.4.	Esborrat i destrucció.....	150
11.14.	PROTECCIÓ DE LA INFORMACIÓ	150
11.14.1.	Neteja de documents.....	150
11.14.2.	Protecció del correu electrònic.....	151
11.15.	PROTECCIÓ DE LES INSTAL·LACIONS	151
11.16.	GESTIÓ D'EXCEPCIONS	151
11.17.	PROTECCIÓ DE DADES DE CARÀCTER PERSONAL	152
11.18.	CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT.....	154
12.	CLÀUSULES GENERALS DE SEGURETAT	156
12.1.	CLÀUSULES D'ADMINISTRACIÓ DE PRODUCTE.....	156
12.1.1.	Gestió d'identitats, autenticació d'usuaris	156
12.1.2.	Autorització dels usuaris als sistemes.....	156
12.1.3.	Inventari d'actius	158
12.1.4.	Configuració de seguretat.....	158
12.1.5.	Manteniment.....	159
12.1.6.	Xifratge de dades.....	159
12.1.7.	Certificats.....	160
12.1.8.	Antimalware.....	160
12.1.9.	Còpies de seguretat.....	160
12.1.10.	Segregació de funcions i tasques	161
12.1.11.	Explotació.....	161
12.1.12.	Protecció dels serveis.....	162
12.2.	CLÀUSULES DE DESENVOLUPAMENT DE PRODUCTE	163
12.2.1.	Clàusula de propietat intel·lectual.....	163
12.2.2.	Desenvolupament segur	163
12.2.3.	Acceptació i posta en servei.....	164
12.2.4.	Dades de proves	164
12.2.5.	Signatura electrònica.....	165



12.2.6.	<i>Pla de traces</i>	165
12.2.7.	<i>Informe de seguretat</i>	165
12.3.	SEGURETAT SISTEMES D'INFORMACIÓ	165
12.3.1.	<i>Àrees separades i control d'accés</i>	165
12.3.2.	<i>Identificació de persones</i>	166
12.3.3.	<i>Condicionament dels espais</i>	166
12.3.4.	<i>Energia elèctrica</i>	166
12.3.5.	<i>Protecció contra incendis</i>	166
12.3.6.	<i>Registre d'entrada i sortida d'equipament</i>	166
12.3.7.	<i>Seguretat del perímetre</i>	166
12.3.8.	<i>Protecció de les comunicacions</i>	166
13.	ANNEX 1 INFRAESTRUCTURA WEB	168
13.1.	CATÀLEG D'APLICACIONS	168
13.2.	DESCRIPCIÓ INFRAESTRUCTURA CLOUD PÚBLIC AWS	169
13.2.1.	<i>Introducció Plataforma Hostlamp</i>	169
13.2.2.	<i>Justificació de la migració al cloud a AWS</i>	172
13.2.3.	<i>Arquitectura de xarxa</i>	173
13.2.4.	<i>Arquitectura dels clústers d'aplicacions i de BBDD</i>	176
13.2.5.	<i>Detall del servidor de aplicacions Apache + PHP-FPM</i>	178
13.2.6.	<i>Administració amb salt-stack</i>	178
13.2.7.	<i>Característiques de seguretat/disponibilitat de la infraestructura (AWS)</i>	180
13.3.	REPTES EVOLUCIÓ INFRAESTRUCTURA	188
13.3.1.	<i>Automatització</i>	188
13.3.2.	<i>DevOps</i>	190
13.3.3.	<i>Projectes</i>	191
13.3.4.	<i>Robustesa</i>	197
13.3.5.	<i>Seguretat</i>	201
13.3.6.	<i>Infraestructura</i>	204
14.	ANNEX 2. VOLUMETRIES I DADES	207
14.1.	INTRODUCCIÓ	207
14.2.	ESFORÇ	208
14.3.	SERVEI D'APROVISIONAMENT D'INFRAESTRUCTURA	209
14.3.1.	<i>Infraestructura Webs CMS (PaaS)</i>	210
14.3.2.	<i>Infraestructura Servidors Virtuals Dedicats (IaaS)</i>	211
14.3.3.	<i>Programari com a servei (SaaS)</i>	212
14.4.	LLICÈNCIES I PRODUCTES	212
15.	ANNEX 3: ADINET	213
15.1.	FASE DE LLANÇAMENT	213
15.2.	FASE D'ELABORACIÓ	213
15.3.	FASE DE CONSTRUCCIÓ	214
15.4.	FASE DE TRANSICIÓ	215
15.5.	PLATAFORMA VALID@	216



16. ANNEX 4 : METODOLOGIA AGILE SCRUM@IMI (METODOLOGIA ÀGIL PER A PROJECTES IMI)	218
17. ANNEX 5 : FLUXOS A L'EINA DE TICKETING	219
17.1. MANTENIMENT CORRECTIU.....	219
17.2. MANTENIMENT RECURRENT, EVOLUTIU RECURRENTS I EVOLUTIU IDENTIFICATS.....	219
17.3. SERVEIS TRANSVERSALS DE MANTENIMENT	220
18. ANNEX 6: NORMATIVA DE DESENVOLUPAMENT. DESENVOLUPAMENT A MIDA AL CLOUD PRIVAT DE L'IMI (VERSIÓ 2020)	221
18.1. LLENGUATGES DE PROGRAMACIÓ I FRAMEWORKS PERMESOS	221
18.2. ENTORNS DE DESPLEGAMENT:.....	221
18.2.1. <i>Tecnologies de desenvolupament</i>	222
18.3. DIRECTIUS A SEGUIR EN EL DESENVOLUPAMENT I L'ARQUITECTURA	223
18.3.1. <i>Preparada per a ser Desplegada en Cloud</i>	223
18.3.2. <i>Preparada per a ser desplegada en qualsevol cloud</i>	224
18.4. MODULARITAT I ESCALABILITAT	225
18.4.1. <i>Arquitectura Modular</i>	225
18.4.2. <i>Publicació a l'API Manager</i>	226
18.4.3. <i>Frontals o Clients (Presentació)</i>	226
18.4.4. <i>Estructura multi-idioma</i>	227
18.5. DIRECTIVES A TENIR EN COMPTE TANT EN L'ADQUISICIÓ DE SOFTWARE COM EN EL DESENVOLUPAMENT A MIDA.....	227
18.5.1. <i>Traçabilitat</i>	227
18.5.2. <i>Components de software lliure</i>	227
18.5.3. <i>Stages</i>	227
18.5.4. <i>Usabilitat</i>	228
18.5.5. <i>Eficiència</i>	228
18.5.6. <i>Seguretat de l'aplicació</i>	229
18.6. QUALITAT	231
18.6.1. <i>Codi</i>	231
18.6.2. <i>Qualitat de codi</i>	231
18.6.3. <i>Qualitat del producte final</i>	232
18.7. METODOLOGIA DE DESENVOLUPAMENT	234
18.8. REPOSITORI DE CODI	234
18.9. CONSTRUCCIÓ I DESPLEGAMENT.....	235
18.10. LLICÈNCIES.....	235
19. ANNEX 7: NORMATIVA PYTHON	236
19.1. INTRODUCCIÓ	236
19.2. ARQUITECTURA BÀSICA	236
19.2.1. <i>Codi</i>	236
19.2.2. <i>Components</i>	237
19.2.3. <i>Construcció i desplegament</i>	237
19.3. SEGURETAT	237



19.4.	DIRECTRIUS DE DESENVOLUPAMENT	237
19.4.1.	<i>Implementacions</i>	240
19.5.	DIRECTRIUS DE SEGURETAT	242
19.5.1.	<i>Implementacions</i>	243
19.6.	DIRECTRIUS D'INSTRUMENTACIÓ	243
19.6.1.	<i>Implementacions</i>	243
19.7.	DIRECTRIUS DE QA (DESENVOLUPAMENT).....	243
19.7.1.	<i>Implementacions</i>	244
19.8.	DIRECTRIUS DE DOCUMENTACIÓ	244
19.8.1.	<i>Implementacions</i>	245
20.	ANNEX 8: DRUPAL	246
20.1.	GUIES DESENVOLUPAMENT DRUPAL.....	246
20.1.1.	<i>Nomenclatura paquets PHP Ajuntament</i>	246
20.1.2.	<i>Rutes i menús d'administració</i>	247
20.1.3.	<i>Guia estil codi PHP a Drupal</i>	248
20.1.4.	<i>Gestió de codi obsolet</i>	255
20.1.5.	<i>Variables Entorn</i>	256
20.1.6.	<i>Sincronització de configuració(Config Ignore, Config Split, etc)</i>	257
20.1.7.	<i>Gestió redireccions per idioma arrel</i>	262
20.2.	ENTORN LOCAL. DDEV.	263
20.2.1.	<i>Instal·lació</i>	264
20.2.2.	<i>Montar entorn nova web amb ddev</i>	264
20.2.3.	<i>Importació de BBDD (per a webs existents)</i>	265
20.2.4.	<i>Dades importants</i>	266
20.2.5.	<i>Comandes útils</i>	266
20.2.6.	<i>Migració DrupalVM/Aquia Dev Desktop a DDEV</i>	266
21.	ANNEX 9: INFORMACIÓ AMPLIADA QUE ES POSA A DISPOSICIÓ (SOTA DEMANDA)	268
22.	ANNEX 10: DUBTES I ACLARIMENTS.....	268
22.1.	CORREU ELECTRÒNIC DE SUPORT.....	268
22.2.	SESSIÓ INFORMATIVA	269



GLOSSARI

Aplicació informàtica: programa informàtic dissenyat com a eina per permetre a l'usuari realitzar una o diverses tasques.

Acord de nivell de servei: acord escrit entre el proveïdor del servei i el client amb l'objectiu de fixar un nivell acordat per la qualitat del servei.

Actualització tecnològica: adaptació a noves versions de tecnologia base.

ADINET: metodologia de desenvolupament de projectes pròpia de l'Ajuntament de Barcelona per aconseguir l'assegurament i manteniment dels sistemes d'informació, garantint la qualitat, abast, termini i cost prèviament acordats.

Arquitectura: conjunt de patrons que proporcionen un marc definit i clar per interactuar amb el codi font de desenvolupament de software.

Backlog: llista d'ítems de treball (normalment requeriments en format d'històries d'usuari) per a un producte desenvolupat utilitzant el marc de treball Scrum.

Canvi normatiu: canvi produït en la normativa legal que afecta a l'objecte del contracte i que requereix d'accions d'adaptació dels sistemes.

Connexió LAN-to-LAN: servei de transmissió de dades punt a punt basat en un protocol IP, que permet connectar dues seus d'un mateix client.

Consulta bloquejant: consulta de tipus funcional resultant d'un bloqueig en l'operativa habitual.

Consulta normal: consulta de tipus funcional sense bloqueig en l'operativa habitual.

Èpica: contenidor d'ítems del backlog que serveix per fer un seguiment a alt nivell de la realització d'un conjunt de funcionalitats més petites (ítems en forma d'història d'usuari).

Equip de desenvolupament: és el conjunt de professionals que realitzaran totes les activitats de definició, construcció, prova i desplegament del producte. La seva mida acostuma a estar entre 3 i 9 persones.

Equip Scrum: és la cèl·lula operativa d'un projecte Scrum. Consta de l'equip de desenvolupament, el Product Owner i el Scrum Master.

Evolutiu identificat: realització de les tasques necessàries per incorporar noves funcionalitats per tal d'adaptar l'objectiu global de l'aplicació a nous requeriments.

Evolutiu recurrent: adequació constant dels sistemes i processos a noves necessitats i peticions de millores funcionals.



Firewall: part d'un sistema o xarxa que està dissenyat per bloquejar l'accés no autoritzat, permetent al mateix temps comunicacions autoritzades.

Història d'usuari: funcionalitat de mida reduïda i rellevant per l'usuari. S'acostuma a identificar amb el format canònic: Com <rol> vull <nom de funcionalitat> per <benefici per l'usuari>.

Incidència: defecte o fallida que bloqueja l'aplicació o els processos de funcionament habituals.

Increment del producte: resultat de l'sprint que ha de ser potencialment lliurable al client. Això vol dir que com a mínim ha d'estar provat i validat pel client en un entorn realista, i que ha de contenir tots els components de la solució, com el codi, però també les proves i la documentació.

Llicència de software: contracte entre el llicenciador (titular dels drets d'explotació) i el llicenciatari (usuari consumidor) del programa informàtic, per utilitzar el software complint una sèrie de termes i condicions.

Manteniment correctiu: resolució d'incidències i/o problemes identificats a les aplicacions per part dels usuaris que provoquen un mal funcionament d'aquestes.

Manteniment recurrent: l'adequació de les aplicacions als constants canvis en els sistemes i processos, a les noves necessitats, peticions de millores funcionals, formacions i transicions.

Metodologia Agile: metodologia àgil de desenvolupament de projectes pròpia de l'Ajuntament de Barcelona.

Mòdul: conjunt de funcionalitats amb una coherència funcional. Els mòduls poden descriure's al backlog com un conjunt d'èpiques.

Parametrització: capacitat de personalització del sistema permetent que es puguin modificar aspectes puntuals del seu funcionament sense necessitat de realitzar desenvolupament evolutiu.

Pas a producció: procés a través del qual les aplicacions o evolutius desenvolupats es transfereixen al computador productiu destí amb l'objectiu de ser utilitzats per l'usuari final.

Penalització: import o percentatge de sanció que s'aplica en cas d'incompliment d'un o més acords de nivell de servei.

Pla de lliuraments (release plan): descripció de l'estratègia de lliuraments del producte al client. Un lliurament és el resultat de la descomposició d'una part del backlog en sprints.

Problema: origen d'una o més incidències de les que es desconeix la causa. Una vegada una o varies incidències s'agrupen en un problema, es centralitza l'anàlisi i la seva resolució.

Producte: sistema informàtic que es crea o es manté.



Product Owner (PO): segons Scrum és el rol que gestiona el producte, representant al client i marcant les prioritats per maximitzar el valor lliurat. Aquest rol pot definir els ítems del backlog i validar-los, o bé delegar aquesta funció en alguna altra persona, típicament membres de l'equip de desenvolupament.

Proves funcionals: prova basada en l'execució, revisió i retroalimentació de les funcionalitats prèviament dissenyades per a l'aplicació que busquen avaluar que l'aplicació conté les funcionalitats que s'han especificat.

Proves UAT: proves funcionals definides i que es realitzen de forma conjunta amb els usuaris referents i on es verificarà que els requeriments funcionals definits es compleixin.

Proves UA AM: proves funcionals definides i executades de forma prèvia a les proves UAT, aprovades a l'inici del desenvolupament, dissenyades i executades pels Serveis Transversals de Manteniment (STM).

Qualitat tècnica: subservei de manteniment recurrent que inclou tasques de millora dels sistemes o de les integracions amb tercers, per ser incorrectes o estar incomplets, i tasques de manteniment preventiu i prefectiu.

Requeriment: necessitat documentada sobre el contingut, forma o funcionalitat d'una aplicació informàtica.

Reunió de Kick-off: reunió de llançament de projecte.

SAU: Servei d'Atenció a l'Usuari.

Serveis d'aplicació: l'agrupació funcional d'un o més sistemes TIC i tasques associades que faciliten els processos de negoci de l'organització. Aquests serveis estan governats pel responsable de servei de l'IMI.

Serveis d'aplicació totalment externalitzats: serveis d'aplicació on la figura del responsable de servei està inclosa en el contracte i és responsabilitat de l'adjudicatari, que governarà el servei en la seva totalitat.

Serveis del contracte: conjunt de serveis inclosos en el contracte, amb el seu corresponent abast: manteniment correctiu, manteniment recurrent, evolutius identificats, serveis transversals de manteniment i aprovisionament d'infraestructura.

Serveis Transversals de Manteniment (STM): serveis que tenen com a objectiu l'assegurament de la qualitat, la documentació, el govern i, en general, el correcte desenvolupament del contracte

Transició: està format pel període de Recepció i de Devolució. El període de recepció comença en el moment en què es formalitza el contracte, es gestiona per cadascun dels serveis d'aplicacions i el seu calendari, i finalitza en el moment en què el nou adjudicatari inicia la prestació de cada servei. I el període devolució comença en el moment en què



l'adjudicatari inicia les tasques de transferència de coneixement al futur proveïdor del servei o a l'IMI, i finalitza a la data de finalització del contracte.

Volumetries: informació estadística propietat de l'IMI dels diferents serveis objecte del plec per poder realitzar l'exploració de dades.



1. INTRODUCCIÓ

L'Institut Municipal d'Informàtica (en endavant, IMI) és l'organisme autònom de l'Ajuntament de Barcelona que té com a objectiu subministrar tots els serveis de les tecnologies de la informació i comunicació (TIC) de l'Ajuntament de Barcelona i les empreses públiques que en depenen.

Entre les seves funcions està el desenvolupament, manteniment i evolució de solucions TIC eficients i productives per a la ciutadania i els empleats municipals.

La naturalesa d'aquestes aplicacions és diversa, atenent a factors com la criticitat, el volum d'usuaris, el volum de dades i l'entorn funcional i tecnològic sobre els quals operen.

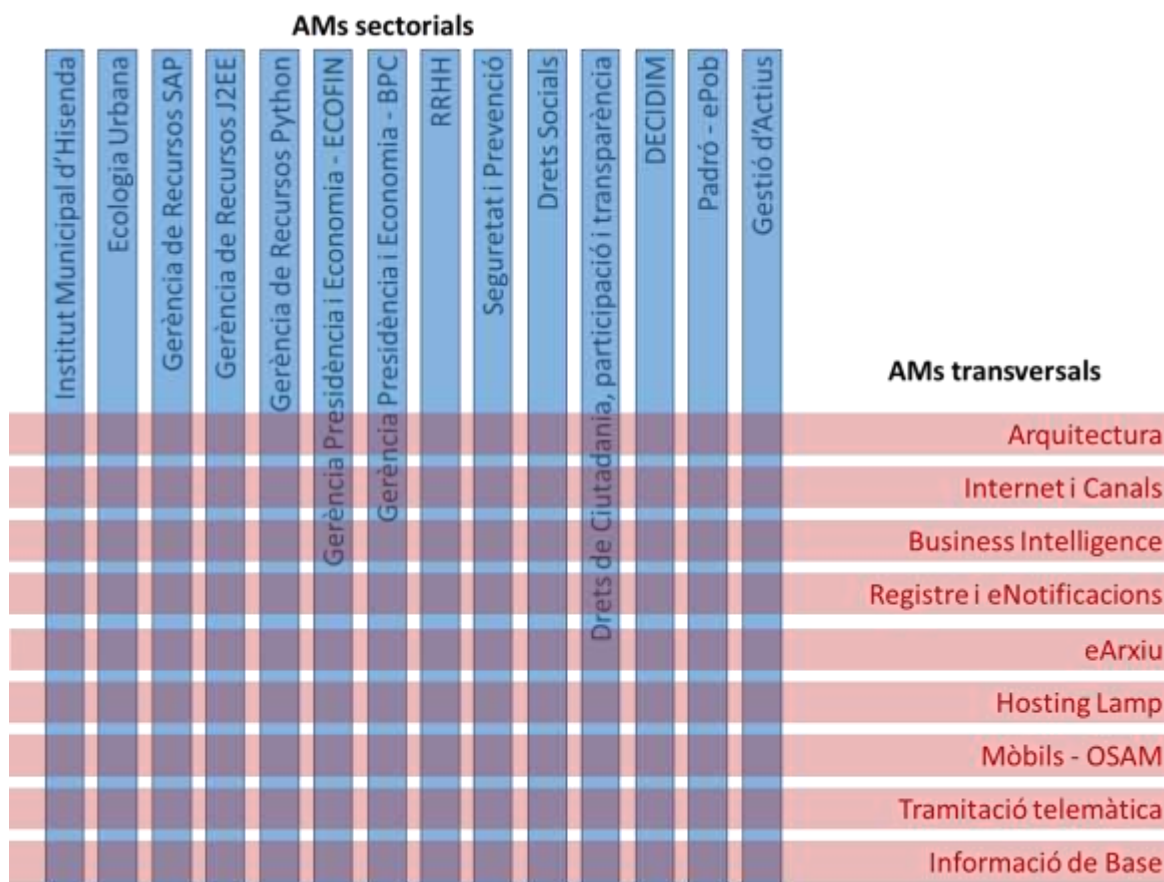
Aquestes aplicacions requereixen de manteniment, suport i desenvolupament de funcionalitats fruit de noves necessitats sorgides a les diferents àrees.

La direcció de Serveis de Desenvolupament de l'IMI té com a missió el desenvolupament, manteniment i evolució de solucions de programari TIC eficients i productives per a la ciutadania i els empleats municipals amb la millor adequació d'abast, qualitat, costos i terminis, seguint l'arquitectura corporativa definida i conservant el coneixement dins l'Ajuntament. Per aconseguir-ho es treballa en dues grans línies:

- En el manteniment i evolució de Solucions existents: Gestionar la demanda de correctius i petits evolutius per complir amb els acords de nivells de servei i supervisant i controlant als proveïdors.
- En el desenvolupament de grans evolutius i noves solucions: Executar el cicle de vida complet del projecte: estudi de viabilitat i pressupost, presa de requeriments, anàlisi i disseny funcional i tècnic, desplegament i posada en marxa.

La contractació dels serveis de gestió de manteniment d'aplicacions informàtiques (en endavant, AM) de l'IMI segueix, des de les licitacions del contractes l'any 2018, una estratègia de concentració dels diferents contractes dels serveis de manteniment de les àrees en dos eixos diferenciats:

- **AMs transversals**, formats per un conjunt d'aplicacions que afecten a diferents àrees de negoci de l'IMI i poden donar servei tant a l'IMI com a l'Ajuntament i als seus ens.
- **AMs sectorials**, que abasten un conjunt d'aplicacions que afecten a una sola àrea de negoci.



Aquestes aplicacions requereixen de manteniment, suport i desenvolupament de funcionalitats fruit de noves necessitats sorgides a les diferents àrees.

Aquest contracte correspon a l'AM transversal de Hosting Lamp.

El Departament de Canals Digitals de la Direcció de Comunicació de l'Ajuntament de Barcelona opta per l'ús de tecnologies LAMP, en concret Drupal i Wordpress, per a la creació dels seus webs.

Mitjançant el present plec per a la contractació dels serveis de gestió de manteniment d'aplicacions informàtiques (AM), l'IMI té com a objectiu la contractació de la infraestructura, els serveis de manteniment i govern, i dels serveis de manteniment de seguretat global dels webs LAMP allotjades a cloud públic.



2. OBJECTE

L'objecte del procés de licitació és la contractació dels serveis d'aprovisionament d'infraestructura, serveis de manteniment i govern, i manteniment de seguretat de webs LAMP de la Direcció de Comunicació de l'Ajuntament de Barcelona.

Que es concreta en aquestes grans línies:

- Proveir Infraestructura de cloud públic (AWS Amazon Web Services o similar)
- Administració de la infraestructura i evolució de la plataforma
- Evolutius de les eines de govern, d'automatització i d'autoprovisió (Python)
- Manteniment webs LAMP Drupal/Wordpress (actualitzacions de seguretat, QA, rendiment,...)
- Suport a campanyes crítiques (mercè, cavalcada, inscripcions prèvies,...)
- Gestió projecte/contracte

I té aquests objectius:

- disponibilitat webs i infraestructura
- agilitat de desplegament
- Escalabilitat en projectes i serveis, donat l' Alt volum desplegaments i de peticions
- Simplificar la infraestructura: netejar el deute tecnològic, millorar les configuracions de seguretat i rendiment, actualitzacions tecnològiques, passar a serveis gestionats
- Autonomia i verificació automàtica: empoderar el desenvolupador; tenir autonomia empodera i dona una sensació de control i responsabilitat (Sygox/SSHail/checklist) que motiva l'equip tècnic que desitja que la seva aplicació funcioni
- Reduir errors: La transmissió d'una tasca entre equips introdueix soroll i confusions, si es pot fer directament la tasca s'eliminen els errors de transmissió de la mateixa i s'incrementa la fiabilitat.
- Reduir el temps de resolució de les incidències: Automatització de tasques habituals
- Optimització de costos: dimensionament adequat, revisar ineficiències, vital quan es consumeix/factura com a servei.

El plec de prescripcions tècniques per al manteniment i evolució d'aquests sistemes, detalla els requeriments tècnics, operatius i de gestió que s'hauran de complir en la prestació d'aquest servei.

El manteniment i evolució d'aplicacions informàtiques (AM) consta dels següents serveis, descrits en el present plec de prescripcions tècniques:

1. Servei de manteniment correctiu
2. Servei de manteniment recurrent (inclou el servei de transició)
3. Servei d'evolutius identificats (no aplica en aquest contracte)
4. Servei d'evolutius recurrents
5. Servei transversals de manteniment (STM) (Inclou el servei de "Coordinació de la transició del servei")
6. Servei d'aprovisionament d'infraestructura



3. ABAST

Els serveis a prestar que apliquen al present procés de contractació pública, són els que s'indiquen en el següent quadre:

Serveis del contracte	Subserveis inclosos	
Manteniment correctiu	Gestió d'incidències	
Manteniment recurrent	Canvis normatius	
	Actualitzacions tecnològiques	
	Qualitat tècnica	
	Avaluació de noves necessitats	
	Acompanyament i recepció de nous projectes	
	Millores funcionals i parametrització	
	Formació	
	Sondes de monitorització i consultes preventives	
Transició		
Desenvolupament d'evolutius identificats		
Evolutius recurrents	Evolutius motivats per canvis normatius	
	Evolutius motivats per actualitzacions tecnològiques	
	Evolutius motivats per qualitat tècnica	
	Evolutius motivats per millores funcionals i parametrització	
Serveis Transversals de Manteniment (STM)	Operació	<i>Serveis de coordinació tècnica i funcional</i>
		<i>Planificació, seguiment i control del servei</i>
		<i>Assegurament de la qualitat</i>
		<i>Coordinació incidències i problemes</i>
		<i>Supervisió de sondes de monitorització i consultes preventives</i>
		<i>Supervisió, planificació i reporting de processos batch</i>
		<i>Administració de Sistemes</i>
	Suport	<i>Help Desk</i>
		<i>Suport funcional</i>
		<i>Suport tècnic</i>
		<i>Coordinació de la documentació</i>
	Gestió del canvi	<i>Comunicació</i>
		<i>Coordinació de la transició del servei</i>
	Gestió del contracte	<i>Reporting</i>
		<i>Indicadors del servei</i>
		<i>Gestió de riscos</i>
	Llicències i productes	



Servei d'aprovisionament d'infraestructura	<i>Infraestructura Webs CMS (PaaS)</i> <i>Infraestructura Servidors Virtuals Dedicats (IaaS)</i> <i>Programari com a servei (SaaS)</i> <i>Suport a la infraestructura</i>
--	--

A continuació es detallen les tasques i obligacions del proveïdor respecte a cada servei.

Consideracions sobre la imputació d'hores

Cada treballador/a del contracte del proveïdor haurà d'imputar les seves hores incorregudes en cada tiquet individual de l'eina de ticketing (manteniment correctiu, manteniment recurrent, evolutius identificats, evolutius recurrents i Serveis Transversals de Manteniment (STM), i Suport a la infraestructura).

Totes les imputacions del mes hauran d'estar introduïdes i revisades pel responsable de l'adjudicatari abans del 5è dia laborable del mes següent. A banda de les imputacions haurà complimentar-se en l'eina de ticketing la informació de detall dels tiquets modificats en el mes i el seu estat. En cas contrari, s'aplicarà l'ANS corresponent de tancament i qualitat. Qualsevol modificació a partir d'aquest punt serà a criteri i sota validació del responsable del contracte IMI, no acceptant-se en cas contrari.

No s'acceptaran alteracions en les imputacions de mesos passats ja facturats. En cas contrari, s'aplicarà l'ANS corresponent. Qualsevol modificació serà a criteri i sota validació del responsable del contracte IMI, no acceptant-se en cas contrari.

El proveïdor haurà de planificar i balancejar feines online i offline amb l'objectiu de no veure afectada la seva productivitat davant incidències de comunicació o infraestructurals amb l'IMI.

El present contracte s'executarà pel sistema de determinació de preus és mitjançant preus unitaris, per tant l'import de licitació actuarà com a límit de despesa. L'import del contracte es consumirà entre tots els serveis i subservei previstos, d'acord amb les necessitats.

L'adjudicatari té l'obligació de desar els arxius generats (documentació i altres) als diversos repositoris que l'IMI indiqui (GitLab, carpetes departamentals, a la pròpia eina de ticketing, etc.).

3.1. Manteniment correctiu

El servei de manteniment correctiu fa referència a les tasques que s'executaran de forma continuada amb la finalitat de garantir la disponibilitat i el correcte funcionament de les aplicacions i el seu ús per part dels usuaris (veure a l'Annex 5, el flux actual de manteniment correctiu a l'eina de ticketing).



L'objectiu dels treballs de manteniment correctiu és identificar i eliminar els possibles defectes o fallides del propi sistema o d'integracions amb sistemes externs, que bloquegen les aplicacions o els processos de funcionament.

3.1.1. Gestió d'incidències

El servei de manteniment correctiu inclou les activitats de recepció de la incidència, diagnosi, correcció del codi i/o l'actualització de la configuració existent, proves necessàries per la posada en productiu de les modificacions i formació tècnica o funcional, facilitant així la transferència de coneixement relacionat amb l'activitat del manteniment correctiu.

El volum d'activitat associat a aquest servei s'ha estimat tenint en compte l'històric de contractes anteriors. El detall de les volumetries s'especifica en l'Annex 2 del present plec.

És responsabilitat de l'adjudicatari complimentar a l'eina de ticketing de forma detallada la informació del manteniment correctiu (origen i causa de la incidència, anàlisi i la seva resolució). Igualment, serà responsabilitat de l'adjudicatari, mantenir actualitzat l'estat del ticket en l'eina de gestió d'incidències (actualment HPSM), incloent el **tancament**, en cas que aquestes no es creïn directament a l'eina de ticketing.

L'IMI podrà:

- Passar a estat "tancat"/"cancel·lat" a l'eina de ticketing, els tiquets no resolts en més de 20 dies laborables o el número de dies que l'IMI determini.
- Passar a estat "in progress" els tiquets assignats a un estat que interromp el comptador d'ANS (p.ex. els estat pending) tant per no estar justificats, com per estar en aquell estat més de 3 dies laborables o el número de dies que l'IMI determini; i limitar el número de vegades que un mateix tiquet pot estar en estat "pending".

A nivell de resolució es podran crear "**problemes**", en el cas que hi hagi una incidència que es produeix de forma repetitiva, de manera que resolent el problema es tanquin totes les incidències associades, o bé quan sigui un tipus d'incidència que requereixi una solució complexa. En el cas d'identificar-se la necessitat de crear un problema, l'adjudicatari presentarà la justificació a l'IMI, la qual haurà de ser **validada per l'IMI** per certificar la creació del problema. En el cas de no ser aprovada, el problema s'anul·la i es retorna a l'estat d'incidència.

En el moment de la creació d'un problema, l'adjudicatari haurà de comunicar i justificar la data prevista de resolució de problema, que haurà de ser de dos mesos màxim. Únicament en el cas dels problemes més complexos, que afectin a l'operativa del servei de l'Ajuntament, la seva resolució màxima no podrà ser superior a 3 mesos.

Els problemes es facturen a la tarifa de manteniment correctiu. Veure detall de coordinació de problemes a l'apartat "3.5.1.4 Coordinació incidències i problemes" del present plec .

El tractament d'incidències serà classificat amb la subtipologia de "Gestió d'incidències".



El licitador haurà de presentar una proposta de diagrama de flux de manteniment correctiu i els procediments associats. Es valorarà la claredat del diagrama plantejat i que els procediments siguin el més complerts possibles i aplicables en un entorn com el de l'IMI.

3.2. Manteniment recurrent

El servei de manteniment recurrent fa referència a l'adequació i petites modificacions de les aplicacions als constants canvis en els sistemes i processos, a les noves necessitats i a les peticions de millores funcionals (veure a l'Annex 5, apartat 17.2, el flux actual de manteniment recurrent a l'eina de ticketing).

El volum d'aquests serveis s'ha calculat tenint en compte l'històric. El detall de les volumetries s'especifica en l'Annex 2: Volumetries del present plec.

El seu increment o decrement pot ser motiu d'ampliació o de disminució del contracte segons allò previst a l'apartat de possibles modificacions del contracte per causes precises o previstes del plec de clàusules administratives particulars.

Tots els manteniments atesos per aquest servei, en el transcurs del desenvolupament del contracte, hauran de complir el següent flux de tramitació, excepte el subservei de Transició en el cas de Recepció:

- L'IMI comunica a l'adjudicatari el manteniment recurrent a realitzar i la seva prioritat.
- L'adjudicatari realitza una anàlisi tècnica prèvia del recurrent i comunica a l'IMI, en el format que l'IMI determini, la informació de la valoració, l'esforç necessari i la data de lliurament en què es compromet a lliurar el recurrent a l'IMI. Les hores de valoració s'imputaran en el tiquet de l'eina.
- Per a tots els subserveis de manteniment recurrent, excepte el subservei "Avaluació de noves necessitats", en cas que el manteniment recurrent al final no es realitzi i només s'hagi valorat, el tiquet amb les seves imputacions d'hores es cancel·larà i es modificarà com a servei de contracte de Serveis Transversals de Manteniment (STM), tasca de suport tècnic.
- L'IMI analitzarà la valoració i la data presentada pel proveïdor:
 - o **L'adjudicatari no podrà imputar hores fins que la tasca no hagi estat acceptada per l'IMI (excepte les necessàries per a la valoració)**
 - o En el cas d'estar d'acord podrà donar aprovació a l'inici dels treballs.
 - o En cas d'identificar alguna necessitat d'aclariment, s'iterarà amb l'adjudicatari fins resoldre'l.
 - o En cas que la valoració i estudi previ realitzats manifestin mancances de qualitat o faltant no identificats correctament per l'adjudicatari, la revisió i correcció de les mateixes correrà a càrrec de l'adjudicatari en concepte de garantia i sense cost per a l'IMI, a banda de l'aplicació del corresponent ANS.
 - o La data d'entrega planificada proposada per l'adjudicatari haurà de tenir present tots els serveis inclosos al recurrent i les seves respectives dates intermèdies. L'adjudicatari la presentarà i explicarà a l'IMI per obtenir la seva validació.



- La coordinació amb tots els agents implicats en cada recurrent serà responsabilitat de l'adjudicatari.
- En cas de no ser acceptada per l'IMI, tant per valoració (estimació d'esforços necessaris), com per planificació, el proveïdor estarà obligat a presentar una nova valoració/planificació, i estarà subjecte a l'ANS "Anàlisis i planificació de peticions (Plani)" (veure apartat de Serveis de Manteniment Recurrent).
- El procés d'aprovació serà conjunt IMI-proveïdor, on es fixarà la data de lliurament. Si un cop aprovada la data de lliurament hi hagués un canvi de prioritat que afecta un manteniment recurrent, l'IMI, d'acord amb el proveïdor, podrà re-planificar la data de lliurament del manteniment recurrent afectat.
- De la mateixa manera si s'identifica un canvi d'abast en el recurrent no imputable a l'adjudicatari, l'IMI, d'acord amb el proveïdor, podrà demanar la revaloració i re-planificació de la tasca.

L'IMI es reserva el dret de contrastar les valoracions realitzades per altres mitjans. En concret i en el que es refereix a tasques tècniques o d'arquitectura l'IMI compta amb una àrea que se n'ocupa de les qüestions comuns i de suport transversal als desenvolupaments. En cas de conflicte o discrepància en l'enfoc de solucions o en l'estimació dels esforços a dur a terme, el responsable del contracte per part de l'IMI, arbitrarà i en cas de no resoldre's prevaldrà la solució i l'estimació realitzada per l'àrea d'arquitectura de l'IMI. En cas que sigui necessari l'IMI podria aplicar el descrit en l'apartat 7.3 Auditories, fins i tot aplicant el règim de faltes i sancions en funció del resultat de les mateixes.

El servei de manteniment recurrent inclou aquests subserveis:

- Manteniments motivats per canvis normatius
- Manteniments motivats per actualitzacions tecnològiques
- Manteniments motivats per qualitat tècnica
- Avaluació de noves necessitats
- Tasques d'acompanyament i recepció de nous projectes
- Millores funcionals i parametrització
- Formació
- Servei post-implantació i estabilització del sistema
- Sondes de monitorització i consultes preventives
- Transició

És responsabilitat de l'adjudicatari complimentar a l'eina de ticketing de forma detallada tant la valoració de cada manteniment recurrent (adicionalment a l'esforç total, es requereix el detall de les tasques principals i el seu esforç), com la informació del manteniment recurrent (origen de la necessitat, anàlisi realitzat, valoració detallada, la seva resolució i tots els **documents generats**). També cal incloure detall a les imputacions realitzades. L'incompliment d'aquesta responsabilitat impedirà el tancament i la facturació del tiquet corresponent fins a la seva subsanació.

A continuació es detallen les tasques a realitzar en cadascun dels subserveis definits. En tots els casos, si el seu volum i complexitat ho requereix, o a petició de l'IMI, es gestionaran



seguint la metodologia ADINET o Metodologia Agile, descrites als Annexes 3 i 4. D'aquesta manera s'assegurarà la definició de les tasques necessàries fins a la seva posada en producció: anàlisi de requeriments, disseny funcional, disseny tècnic i arquitectura d'aplicacions, desenvolupament, proves, proves d'usuari (si s'escau), implantació, i suport post-implantació.

La realització del servei de manteniment recurrent no es pot veure afectada pel volum de feina del servei de manteniment correctiu.

3.2.1. Canvis normatius

Fan referència a aquelles accions necessàries per poder garantir que els sistemes s'adaptin a la legalitat vigent en cada moment.

3.2.2. Actualitzacions tecnològiques

Són les modificacions motivades per actualitzacions a l'entorn en què el sistema opera i que es fan per evitar l'obsolescència tecnològica i el manteniment actualitzat del programari.

Es consideren actualitzacions tecnològiques per exemple, els canvis de configuració del maquinari, el programari base, els gestors de base de dades, comunicacions, etc.

Un exemple d'actualització tecnològica són les actualitzacions de la base de dades MySQL o de la versió del sistema operatiu corporativa dels servidors.

Aquestes accions s'agrupen en 3 grans grups:

- A) Evolució de la infraestructura i l'arquitectura web
- B) Desenvolupament d'evolucius de l'eina de govern SyGox (Python/Django)
- C) Govern seguretat webs LAMP (Drupal/Wordpress)

que es detallen a continuació:

A) Evolució de la infraestructura i l'arquitectura web

Es detalla el manteniment recurrent relacionat amb les actualitzacions tecnològiques que apliquen a l'evolució de la infraestructura i l'arquitectura web.

Són les modificacions motivades per tal d'actualitzar l'arquitectura, racionalitzar la infraestructura, i aplicar millores als sistemes de gestió. Es tracta de tasques orientades a proposar millores de la infraestructura i l'arquitectura, amb l'objectiu de:

- Donar un servei de resposta de pàgines web al ciutadà més ràpid
- Donar un servei d'alta de webs i suport a les incidències més ràpid i barat
- Tenir un millor govern de tots els recursos gestionats
- Millorar la comunicació dels equips tècnics
- Facilitar la portabilitat dels webs entre diferents infraestructures
- Automatitzar tasques habituals



- **Racionalitzar l'ús** de la infraestructura aprofitant més els recursos de les màquines i els serveis.
- **Anàlisi dels costos de infraestructura** per detectar increments sobtats o àrees de millora on es pugui fer un estalvi.
- **Incrementar l'escalabilitat** de les webs fent que siguin resistents a pics.
- **Redundar** o desplaçar els **punts únics de fallada** per facilitar manteniments i millorar la disponibilitat.
- Incrementar la **seguretat** del sistema al millorar les configuracions de les aplicacions i tenir menor nombre de punts a controlar. Fent que sigui fàcil aplicar i desplegar noves polítiques de seguretat de manera segura i àgil.
- **Incrementar la mantenibilitat** del sistema estandaritzant encara més la forma de les aplicacions.
- Incrementar l'**automatització** en el desplegament de configuracions.

A continuació es mostra el detall de les tasques principals incloses al servei:

Automatització: Aplicació de la infraestructura com a Codi (IaC)

Automatització progressiu de les tasques més habituals, analitzant quines són les més freqüents, sempre que l'anàlisi de benefici/cost ho justifiqui.

L'objectiu principal és obtenir un guany de sobirania i control de dades (simplifica la migració de la infraestructura, en cas de voler-se efectuar)

Objectius:

- Reduir errors manuals
- Donar un servei més ràpid
- Possibilitar l'autoprovisionament
- Incrementar la seguretat i control

Optimització Recursos: Consolidació i estandarització de la infraestructura

Consolidació d'aplicacions i base de dades

Tenir els webs en una única infraestructura, anar migrant les antigues,

Realitzar un inventariat al dia

Optimitzar ús de BD de les aplicacions Drupal (revisió Redis / memcache)

Objectius:

- Estandarització i possibilitat d'aplicar pràctiques "industrials" en la gestió de la infraestructura (reducció de cost de servei i infraestructura)
- Possibilitat d'escalar millor i donar cabuda a augments de rendiment



Documentació

Millorar procediments de documentació per tal de que estigui més actualitzada i sigui més útil a l'operativa diària, i fer procediments fàcilment actuables per un operador sense pràcticament coneixements de la infraestructura.

Monitorització

Proposta de millores als sistemes de monitorització de tots els serveis, actualment es realitza amb Nagios i Grafana. Actualitzar les plataformes de monitorització, avaluar periòdicament (com a mínim mensualment) l'addició de nous registres a mesurar, integració de noves alertes, etc.

En aquest apartat també s'inclouen aquells aspectes de monitorització proactiva que permetin detectar les incidències l'abans possible, per exemple: retards inexplicables en un servei (pot indicar que alguna configuració està malament), aparició de timeouts (pot indicar que no es té accés a algun recurs), increment inexplicable de connexions de sortida (pot indicar que el sistema ha tingut una intrusió i està compromès), canvis en els fitxers de sistema que no han realitzats els administradors (infecció), etc.

Rendiment

Proposta d'iniciatives orientades a millorar el rendiment. Avaluacions puntuals globals de rendiment per detectar on s'han de focalitzar els esforços. Aplicació de les millores, proves de concepte de noves solucions, comparatives de millora de rendiment. Sol ser habitual mitjançant la incorporació de memòria cau a varis nivells.

Seguretat: Informació sobre vulnerabilitats vigents

Mantenir-se informat sobre incidències de seguretat en els components de l'ecosistema Web utilitzat, tant a nivell de sistema operatiu, programari base, i gestors de contingut Drupal i Wordpress. Proposar i aplicar iniciatives que enforteixin la seguretat de configuracions i webs enfront als nous vectors d'atac.

Fer seguiment de les incidències de seguretat obertes de les quals encara no s'ha desenvolupat un pegat o actualització de seguretat.

Seguretat: Revisió i actualització de seguretat de les guies de bastionat:

Aquesta tasca es refereix a la millora proactiva de la configuració de seguretat: revisió en profunditat de les polítiques de seguretat actuals, i propostes de millora a les guies de seguretat i bastionat usades per securitzar la infraestructura.

Aplicar les noves actualitzacions a les guies bastionat que al seu torn proporcioni el departament de seguretat de l'IMI a tots els servidors productius.

Seguretat: Revisió de seguretat dels servidors



Aplicació de les guies de bastionat i dels nous estàndards als servidors actuals. Cal revisar que els servidors compleixin la seguretat acordada (ISO 27001, ENS, requeriments de l'IMI), identificant aquells que per la seva obsolescència, o per no haver estat gestionats per l'adjudicatari fins al moment, no compleixen els criteris especificats a les guies.

Coincidint amb la revisió periòdica de seguretat (que es fa com a mínim trimestralment), caldrà realitzar un informe de l'estat de seguretat de cadascun dels servidors, conforme a les guies, per indicar quina versió de guia apliquen, i aspectes a revisar identificats.

Per tots els punts identificats que a criteri de l'IMI siguin de criticitat mitja o alta, caldrà corregir-ho, i presentar un informe final de totes les correccions fetes i l'estat final de la seguretat dels servidors.

També inclou l'actualització de tot el programari base dels servidors, i desinstal·lació de peces de programari no usades.

En cas d'incidència de seguretat greu durant l'execució del contracte, com per exemple la notificació d'una vulnerabilitat greu, **es comunicarà immediatament de manera formal a l'Ajuntament (dins la primera hora des de la detecció)**, i s'aplicaran les mesures d'anàlisi i correctives el més aviat possible (complint els requeriments ANS de l'apartat "8.1.6 : Aplicació de pegats de sistema").

A tal efecte, es detalla a l'apartat 8 : ANS, els criteris pels quals una incidència es considera crítica , i quins plaços màxims (en hores) s'exigeixen per a la seva resolució.

Seguretat: Revisió de seguretat dels webs CM

Aplicació i revisió de l'aplicació als webs de les guies de bastionat i configuracions recomanades. Proposta de millores a les guies de desplegament per facilitar la tasca de nous desplegaments de webs correctament configurades des d'inici. Verificació del compliment de les guies de bastionat pels webs.

Sol ser habitual la revisió d'aspectes primordials com:

- Ús de captcha en formularis de identificació d'usuari
- Recomanació de mòduls de seguiment d'intent d'intrusions
- Evitar l'ús d'usuaris genèrics de drupal/wordpress, evitar l'ús de l'usuari admin
- Separació de les pàgines d'administració fora del web públic
- Configurar i promocionar solucions per l'ús de medis restringits (VPN) per accedir als entorns no productius (desenvolupament i pre-producció) i l'accés al portal d'administració d'entrada de contingut.



Aquestes tasques estan principalment automatitzades amb un script automàtic que revisa el checklist de mínims de qualitat exigida a una web per publicar-se. Caldrà realitzar una execució massiva general a tots els webs (mínim trimestralment) i presentar en un informe un llistat de quins webs no compleixen els criteris, juntament amb el nombre de falles que té cada un.

Seguretat: Integració amb eines de Seguretat Corporatives

Aquesta tasca es refereix al fet que en cas de necessitat, l'equip de Seguretat IMI comuniqui la necessitat de la integració amb una solució de seguretat corporativa de l'IMI.

Un possible exemple podria ser la integració amb la solució de traces de sistema Centralitzades que s'està usant actualment a l'IMI.

Revisió i actualització de procediments

Revisió del repositori de documentació (al Wiki del Gitlab de l'Ajuntament) on hi ha descrits els procediments d'operació habituals, detallant els passos per dur-los a terme, per a referència interna de l'equip de l'adjudicatari.

Es tracta de fer una revisió periòdica per assegurar la coherència i qualitat de la informació del repositori, fer neteja de documents i procediments obsolets, i proposar millores que incrementin la utilitat i la vigència de la informació.

Actualment, hi ha descrits els següents procediments d'operació:

- Suport i manteniment dels sistemes.
- Configuració nous espais web LAMP.
- Des-publicació de webs i des-indexació dels cercadors.
- Configuració i suport per implementar mailing.
- Còpia de portals.
- Configuració de frontals.
- Recuperació de còpia de seguretat.
- Actuacions respecte als virus o atac
- Modificacions de Sistemes (per exemple DNS i registres SPF).
- Migració de webs d'altres proveïdors a la infraestructura LAMP d'aquest contracte.
- Gestió de sondes Nagios.
- Gestió de sondes uptimerobot.
- Seguiment d'indisponibilitats detectades amb les sondes.
- Auditoria de custòdia de certificats.
- Seguiment de vulnerabilitats detectades
- Guia de desenvolupament en Drupal i Wordpress.

A la revisió periòdica, es revisaran tots els procediments per validar que siguin vigents i ben descrits, i s'incorporaran els nous que es considerin. En base a la informació recollida a l'històric de peticions (tiqueting), es podrà identificar les peticions/operacions més habituals, que hauran de correspondre amb algun procediment descrit.



L'adjudicatari doncs, revisarà els procediments, millorarà la descripció i afegirà els nous procediments que hi manquen.

La revisió de completesa dels procediments i la documentació es durà a terme com a mínim trimestralment. La revisió en profunditat es durà a terme com a mínim anualment.

Revisió del pla de contingència

Es dissenyarà i mantindrà el pla de contingència per fer front a diferents possibles problemes habituals que es poden donar: corrupció del sistema, esborrat accidental, intrusió, falta de recursos.

Es revisarà i ampliarà el pla , si s'escau amb nous casos, detallant els passos per dur-lo a terme, els temps de servei previstos, i mancances que es puguin detectar amb propostes de millora.

També es duran a terme pilots de millora de contingència, per exemple recuperar un web en un altre proveïdor de hosting , que permetin a l'IMI millorar la cobertura a possibles incidències i provar les contingències previstes (per exemple per incidències de tipus : discontinuïtat del proveïdor actual, o falta de capacitat del datacenter actual, etc.)

L'adjudicatari, doncs, revisarà els procediments de recuperació, millorarà la descripció, afegirà nous casos si s'escau, farà propostes de sistemes de monitorització proactiva, i mantindrà contingències latents en proveïdors alternatius, justificant el cost/benefici de les millores.

Millorar la configuració de la memòria cau

Aquesta tasca es basa en repassar la configuració actual de memòria cau a tots els nivells (CDN, frontal, intèrpret, CM, bbdd), i proposar millores que portin a una acceleració dels webs i a permetre una millor escalabilitat, alhora que requerir menys recursos de computació.

Actualment es compta amb l'aportació de diferents components de memòria cau, a varis nivells: la infraestructura compta amb frontals a mode de proxy invers amb funcionalitat de memòria cau, i certs dominis estan servits per infraestructures CDN (com Cloudfront), a fi de millorar el rendiment del web i descarregar la infraestructura. La memòria cau del gestor de continguts s'emmagatzema en Redis per evitar guardar-ho a base de dades.

Alhora s'ha de tenir en compte la "frescor" dels continguts a servir, i que s'ha de conservar la capacitat per netejar memòria cau en cas de voler publicar urgentment uns canvis al web.

Optimitzar sistema de còpies de seguretat

Tasques centrades a proposar millores als sistemes de còpies de seguretat, que optimitzin l'espai ocupat i, la integritat, el temps de recuperació , l'automatització i la seguretat. Es



disposa d'un alt volum de webs, servidors i arxius, amb molta rotació de webs temporals, i per tant es generen grans ocupacions de disc que cal mantenir, i vetllar per la seva integritat.

S'inclouen tasques relacionades amb:

- Millora dels procediments i la infraestructura de còpies de seguretat
- Proves habituals de recuperació
- Neteja de còpies de seguretat obsolets
- Automatització de tasques de recuperació
- Vigilància de la integritat
- Minimització de l'impacte en el servei de l'execució de la còpia
- Optimització de l'espai ocupat
- Arxivat "perpetu" d'informació valuosa

Support a la integració contínua per Drupal/Wordpress: incorporació versions antigues

Inclou les tasques de millora del desplegament dels webs Drupal a la infraestructura, en quant a que permetin tenir control de les actualitzacions incorporades pels programadors, i facilitin el diagnòstic de problemes.

Amb la nova incorporació de les últimes versions de drupal, ja es realitza el control de codi i desplegament via GIT, però també es vol optimitzar els procediments de desplegament i incorporar funcions d'integració contínua per versions anteriors de Drupal o Wordpress que no ho permetien, que fa que s'hagin de disposar d'entorns i eines, buscar la millor manera d'implementar-ho.

- Preparació entorn Drupal (noves versions que vagin sortint) amb Composer + procediments de desplegament
- Integració dels entorns amb Git, per passar de desplegament via sFTP a desplegament via Gitlab (amb scripts de suport per programadors que emprin només sFTP, aquest scripts haurien d'utilitzar Git de manera transparent per l'usuari).

Implementar Auto escalat

Es tracta d'un projecte d'evolució de la infraestructura .

Amb l'auto escalat les aplicacions deixaran d'estar vinculades a un servidor i passaran a ser executades a un conjunt de servidors. Pot tractar-se d'escalat horitzontal o vertical, o bé implantar altres tipus de tecnologies , com kubernetes, EKS, o tecnologies serverless de AWS que apliquin.

Com a part del projecte, es volen assolir els següents objectius:

- Racionalitzar l'ús de la infraestructura aprofitant més els recursos de les màquines en condicions normal evitant tenir moltes màquines desocupades.
- Incrementar de l'escalabilitat de les webs fent que siguin resistent a pics.



- Redundar o desplaçar els punts únics de fallada per facilitar manteniments i millorar la disponibilitat.
- Incrementar la seguretat del sistema al millorar les configuracions de les aplicacions i tenir menor nombre de punts a controlar, fent que sigui fàcil aplicar i desplegar noves polítiques de seguretat de manera segura i àgil.
- Incrementar la mantenibilitat del sistema estandaritzant encara més la forma de les aplicacions.
- Incrementar l'automatització en el desplegament de configuracions.

Per tal que cada funcionalitat es pugui aplicar de manera independent a les altres, es plantegen les següents iniciatives:

- Desplegament d'un Cluster Memcached/Redis per guardar les sessions del PHP.
- Desplegament d'un Servei de NFS per posar el codi i les dades de les aplicacions, amb l'objectiu de poder posar en alta disponibilitat els servidors de les aplicacions consolidades.
- Evolució del sistema de Centralització de traces.

Millora dels frontals web

Tasques centrades a la reorganització dels frontals en funció dels nous requeriments.

Els frontals han esdevingut una peça crítica de la infraestructura. Enruten l'entrada de totes les peticions a la infraestructura, i es on es configuren totes les regles de dominis , certificats digitals per encriptació https, i regles de seguretat per prevenir atacs.

Inclou les tasques d'automatització i optimització dels canvis de frontals, com per exemple:

- Separació dels entorns de producció, desenvolupament, i entrada de continguts
- Gestió dels certificats digitals
- Gestió dels dominis
- Enrutament dels dominis i directoris cap al web corresponent
- Configuració de seguretat per prevenir atacs
- Configuració de Redireccions (per exemple, en el cas de webs o URLs obsoletes)
- Configuració de les pàgines d'error , i dels fitxers de control dels robots de Google, yahoo i Bing (robots.txt, sitemap.xml)

Es poden incorporar al servei altres mètodes més proactius a mida que estiguin disponibles, fent un anàlisi del cost/benefici, com per exemple models IA que identifiquen patrons de comportament per identificar anomalies.

Evolucionar l'Arxiu web

Tasques centrades a permetre que es pugui consultar internament webs obsoletes, actualment no publicades, de manera que consumeixin el mínim de recursos humans i d'infraestructura. L'objectiu és que aquests webs , en cas de caldre ser consultats, es puguin



instal·lar durant un temps curt, i disposin de tota la funcionalitat operativa, com si estiguessin en funcionament.

Actualment es disposa d'un arxiu de webs estatificades (tal com es detalla a l'apartat "13.2"), però és molt limitat per què es tracta de webs estatificades, i per tant només són un subconjunt de pàgines i sense la funcionalitat de cerca.

Consolidació de traces de sistema

L'objectiu d'aquesta tasca és l'actualització de procediments de conservació, custòdia, i neteja automàtica de traces de sistema ("logs") segons els estàndards proporcionats per l'IMI.

A banda, també es tracta d'explotar aquests fitxers per obtenir informació útil de cara a l'enfortiment de la seguretat, la correcció d'errors i al control de la càrrega dels frontals.

Per exemple de l'anàlisi d'aquests fitxers de traces del servidor web (en quant a tràfic internet) es pot obtenir detalls de:

- Estadístiques de tràfic no vist: quina càrrega suposen els spiders dels cercadors
- Detall d'atacs de denegació de servei rebuts
- Informació de quin tipus de peticions automatitzades fan els bots maliciosos, per prevenir nous vectors d'atac
- Estudi dels errors 404 més freqüents, per detectar enllaços populars que ja no es dona resposta, o fitxers molt enllaçats que donen molts errors i incrementen la càrrega del servidor (i el volum del fitxer de traces).
- Visites i pàgines vistes a cadascun dels webs, per contrastar amb la informació de google analítics
- Estadístiques de descàrrega de documents, com els PDF

En quant a les traces de sistema, ens ha de permetre identificar inequívocament els accessos i canvis als sistemes i servidors. Per als webs estratègics, ens ha de permetre també identificar quins canvis ha fet cada programador o cada contribuïdor de contingut. Quan sigui necessari es treballarà conjuntament amb els programadors del web per habilitar els mòduls Drupal necessaris per poder disposar d'aquestes traces.

Veure apartat 9.4.5 i 12.2.6 "pla de traces" per més detall sobre el seguiment detallat de fitxers de traces d'accés als sistemes.

Si s'escau, es facilitarà la integració amb l'IMI per consultar/recepcionar els fitxers de traces que aquest requereixi per a la seva consulta i/o conservació.

B) Desenvolupament d'evolutius de l'eina de govern SyGox (Python/Django)

Es detalla el manteniment recurrent relacionat amb les actualitzacions tecnològiques que apliquen al desenvolupament d'evolutius de l'eina de govern SyGox (Python/Django).



Es disposa d'una eina de govern principal feta a mida per a la gestió de la infraestructura i automatització de l'operativa habitual, que s'anomena **SyGox per als webs, i Palàntir-Mobile per a les APPS de mòbil**. Aquestes aplicacions són molt actives i precisen d'un manteniment per tal d'anar cobrint nous requeriments, com poden ser la incorporació de nous proveïdors d'infraestructura a ser gestionats via API, nous procediments que permeten que el peticionari faci autoprovisió, o bé els canvis necessaris derivats de canvis de filosofia d'ús de la infraestructura i que s'han de traslladar a l'eina de govern. Aquestes tenen un manteniment actiu.

La principal eina a mantenir, doncs, és el SyGox, i donat que permet l'acceleració dels procediments i el govern de la infraestructura, serà del màxim interès mantenir-lo evolucionat i obtenir-ne rendiment.

C) Govern seguretat webs LAMP (Drupal/Wordpress)

Es detalla el manteniment recurrent relacionat amb les actualitzacions tecnològiques que apliquen al govern de seguretat dels webs LAMP (Drupal/Wordpress).

Actualment l'Ajuntament de Barcelona compta amb una gran quantitat de webs desenvolupades amb Drupal i Wordpress, i es pot donar el cas que amb el temps algunes d'elles quedin en versions antigues, i que no disposin d'un seguiment per part d'un equip de desenvolupament que les mantingui.

Com que això suposa un risc de seguretat, s'incorpora en aquest contracte el servei de manteniment d'un subconjunt de webs concretes, a fi de mantenir-les actualitzades i vetllar per la seguretat global dels webs CMS.

Es mantindrà una llista de les webs concretes responsabilitat de l'adjudicatari, a fi de que quedin clares les webs que ha de mantenir i actualitzar aquest durant el contracte. Els webs a mantenir a nivell de programació, estaran allotjades a la infraestructura gestionada en aquest propi contracte.

Per tant, les funcions a cobrir són:

- Dur a terme actualitzacions de seguretat d'una llista de webs pactada amb l'IMI (correspon als webs que ja no tenen manteniment de proveïdor)
- Estar informat de problemes de seguretat i actualitzacions de seguretat (o "pegats") de Drupal i Wordpress
- Mantenir inventari de versions de la totalitat de webs CMS inclosa al contracte
- Mantenir l'eina per poder dur a terme el seguiment centralitzat i automatitzat de les versions dels Drupal/Wordpress, mòduls instal·lats, usuaris de gestió, i en general tot el que pugui afectar a la seva seguretat.

3.2.3. Qualitat tècnica



Són les modificacions motivades per implementacions incomplertes o incorrectes dels sistemes o de les integracions amb tercers, tant a nivell tècnic com de funcionalitats requerides pels usuaris.

Normalment la seva existència suposen una càrrega en tasques de manteniment repetitives i improductives per tal de cobrir aquestes mancances.

Un exemple de dèficit de qualitat tècnica és la necessitat de revisió manual de tasques o processos automàtics per la seva manca de fiabilitat o estar incomplerts.

Un altre exemple és la manca de funcionalitats d'administració per part de l'usuari en la gestió autònoma del sistema.

En la mateixa línia, un dels objectius d'aquest contracte és la reducció del nombre d'incidències històriques que es produeixen en els sistemes, és per això que s'inclouen en l'abast del contracte tasques de manteniment preventiu i perfectiu que han de permetre a l'adjudicatari la reducció de les incidències recurrents:

- Manteniment preventiu. Modifiquen les aplicacions per millorar les seves propietats i facilitar el manteniment futur de les mateixes
- Manteniment perfectiu. Milloren el programari de les aplicacions en qüestions com rendiment, flexibilitat, re usabilitat, etc. L'objectiu d'aquestes millores és reduir el volum d'incidències, millorar el rendiment i facilitar l'ús i les integracions amb altres sistemes.

La realització d'aquests recurrents es planificarà i es prioritzarà d'acord amb el responsable de servei en base a les necessitats del servei. És responsabilitat de l'adjudicatari identificar i proposar la correcció dels casos més destacats i recurrents dins de la prestació del servei.

3.2.4. Avaluació de noves necessitats

De manera general, l'esforç dedicat a valorar cada petició de manteniment recurrent formarà part de la pròpia valoració del manteniment recurrent.

Són les tasques referides a la dotació d'assessoria i coneixement tècnic específic de grans necessitats que requereixin una anàlisi concreta i específica de gran durada en el temps. En aquest subservei s'inclou principalment:

- Respecte a sistemes existents:
 - Enfocament de les possibles solucions a noves necessitats: identificar i analitzar la solució tècnica i funcional per donar resposta a una petició de millora.
 - Anàlisi de processos: anàlisi del procés actual previ a la realització d'un canvi en les aplicacions.



- Estimació de costos d'implementació de les solucions a noves necessitats: establir i valorar en durada, esforç i perfils necessaris les tasques bàsiques.
- Respecte a noves necessitats:
 - Conceptualització de noves necessitats: identificar i analitzar la solució tècnica i funcional per donar resposta a una nova necessitat.
 - Anàlisi de processos: anàlisi dels processos de negoci sobre els quals es requereix realitzar una nova necessitat.
 - Estimació de costos d'implementació de les solucions a noves necessitats: establir i valorar en durada, esforç i perfils necessaris les tasques bàsiques pel desenvolupament d'una nova necessitat.

Les tasques d'avaluació de noves necessitats poden passar també per valorar el cost d'implementació de nous projectes que hagin estat conceptualitzats per tercers, aportant la solució tècnica, costos associats i previsió de recursos i temps per dur-ho a terme.

L'IMI es reserva el dret de contrastar les valoracions realitzades amb altres equips. En concret, i en el que es refereix a tasques tècniques o d'arquitectura l'IMI compta amb una àrea que se n'ocupa de les qüestions comuns i de suport transversal als desenvolupaments. En cas de conflicte o discrepància en l'enfoc de solucions o en l'estimació dels esforços a dur a terme, el responsable del contracte per part de l'IMI, arbitrarà i en cas de no resoldre's prevaldrà la solució i l'estimació realitzada per l'àrea d'arquitectura de l'IMI.

3.2.5. Acompanyament i recepció de nous projectes

Les noves aplicacions desenvolupades durant la vigència del present contracte, una vegada hagin estat lliurades i posades en producció podran ser incloses en l'abast dels serveis licitats en el present procés de contractació. Els costos de suport d'aquestes noves aplicacions es facturaran de manera habitual mitjançant el servei de manteniment recurrent o de correctiu si s'escau.

Dins de les tasques de Manteniment Recurrent l'adjudicatari serà responsable de l'acompanyament, seguiment i recepció dels nous projectes de desenvolupament d'aplicacions de l'àmbit de negoci del present contracte que, tot i havent-se realitzat fora de l'abast del contracte resultant del present procés, finalment, siguin susceptibles d'incorporar-se per al seu manteniment.

Les tasques d'acompanyament i recepció de nous projectes que s'hauran de desenvolupar en cada cas dependran del criteri del responsable del contracte per part de l'IMI, i en funció del projecte i les seves característiques, per exemple nou servei vs. evolució servei en manteniment, etc. Aquestes tasques seran acordades amb l'adjudicatari abans de l'inici de les mateixes per tal de garantir una correcta supervisió i/o recepció del servei.



L'adjudicatari haurà d'ésser el responsable de la vigilància i assegurement de la qualitat durant el procés de construcció de noves aplicacions informàtiques, així com de la recepció de les noves aplicacions susceptibles de ser incloses en l'abast del present plec.

Per tal d'assegurar el servei de recepció i acompanyament de nous projectes, l'adjudicatari haurà d'oferir la informació necessària de l'entorn en el qual s'establirà l'aplicació, per tal d'oferir una visió completa de l'escenari real i evitar, així, possibles incidències futures. Aquest acompanyament i traspàs d'informació es portarà a terme a través de l'assistència de l'adjudicatari, sota demanda de l'IMI al Comitè de Direcció, així com a reunions referents a l'arquitectura i requeriments tècnics, que s'estipulin.

A criteri de l'IMI es podria requerir als adjudicataris de nous projectes la possibilitat de subcontractació de l'adjudicatari del present contracte, per dur a terme aquestes actuacions d'acompanyament i recepció de nous projectes a costa del propi projecte. En aquests casos, s'aplicaran les tarifes d'adjudicació del servei de manteniment recurrent del present contracte. L'avís per part de l'IMI o per l'adjudicatari del projecte, per iniciar les tasques d'aquest subservei s'haurà de rebre amb una anterioritat mínima de dos mesos.

A continuació es detallen les fases i les activitats en les quals serà requerida la participació de l'adjudicatari.

Durant l'execució del contracte d'un nou projecte

Durant el procés de desenvolupament del nou projecte, i des de la data de notificació de l'inici del mateix, l'adjudicatari haurà d'acompanyar i supervisar el correcte desenvolupament segons els estàndards de qualitat exigibles. Aquest subservei requereix **perfils sèniors** exclusivament.

Les tasques a desenvolupar per l'adjudicatari seran, sota criteri de l'IMI i en funció del projecte:

- Reunió prèvia amb el proveïdor assignat i el responsable de l'IMI, per tal d'alinear la solució proposada amb les necessitats funcionals i tecnològiques que requereixen els sistemes d'informació existents i els documents, i els seus formats, a generar durant el projecte i a lliurar a l'AM en la recepció de l'aplicació. Definició dels punts de control i calendari per dur-los a terme.
- Assistència durant l'execució del contracte amb transferència del coneixement de l'entorn tecnològic particular que pugui ser d'interès en el projecte.
- Supervisió a alt nivell de l'arquitectura i entorn tecnològic del projecte.
- Revisió i acceptació del document funcional, tenint present el contingut mínim detallat a l'apartat "3.5.2.4. Coordinació de la documentació".
- Revisió i acceptació del document d'arquitectura i disseny tècnic, tenint present el contingut mínim detallat a l'apartat "3.5.2.4. Coordinació de la documentació".
- Assistència i acompanyament en les reunions i comitès de seguiment, sota demanda de l'IMI.



- Auditories de l'estat del desenvolupament i dels problemes tècnics que es puguin produir, sota demanda de l'IMI.
- Mantenir la comunicació necessària i l'assistència a les reunions i comitès als quals s'ha convocat l'adjudicatari per tal d'oferir la informació requerida.
- Revisió i validació dels plans de proves definits pel projecte de desenvolupament.
- Definició del pla de proves prèvies d'UAT.
- Realització de proves prèvies d'UAT:
 - o Una vegada finalitzada la construcció del nou desenvolupament, l'adjudicatari dins del Manteniment Recurrent realitzarà les proves prèvies d'UAT definides:
 - Si les proves prèvies d'UAT es passen correctament, s'informarà a l'IMI i al proveïdor responsable del projecte de desenvolupament, que tindrà autorització per convocar les proves d'UAT amb l'usuari.
 - Si les proves prèvies d'UAT no es passen correctament, s'informarà a l'IMI i al proveïdor responsable del projecte de desenvolupament dels diferents stoppers (crítics, bloquejants,...) i s'acordaran els ajustos necessaris per a la correcta execució de les proves. Una vegada realitzats els ajustos, ho comunicarà a l'adjudicatari del present contracte, el qual podrà repetir les proves. Aquest procés es repetirà fins que les proves passin correctament i s'informi a l'IMI i al proveïdor responsable del projecte de desenvolupament, que tindrà autorització per convocar i realitzar les seves pròpies proves d'UAT amb l'usuari.
- Definició i execució de proves de regressió en el cas d'una modificació o impacte sobre algun dels serveis sota manteniment, per garantir la correcta continuïtat del servei.
- Suport i coordinació en l'arrencada del nou projecte, fonamentalment si aquest altera o impacta algun dels serveis existents.

Durant la recepció de l'aplicació

Un cop validat el nou projecte, s'inicia el procés de recepció del nou servei o aplicació. Aquesta recepció haurà de comptar, com a mínim, de la següent documentació i accions de traspàs:

- Documentació funcional del projecte (funcional, casos d'ús, maquetes, proves).
- Disseny tècnic, Arquitectura, codi font.
- Formació sobre el funcionament de la nova aplicació, a l'equip receptor i encarregat del seu manteniment.
- Resum de la fase de suport post-implantació i estabilització, si existeix, així com backlog de tasques i millores en cartera o pendents.
- Acta formal d'entrega, convocada per l'IMI, i recepció del projecte.
- Aprovació per part del receptor i en última instància de l'IMI de que el traspàs s'ha efectuat correctament

Si l'IMI ho considera necessari, es pot incloure dins del present subservei, una etapa de shadowing o paral·lel realitzada per l'adjudicatari del present contracte, en fase de suport



del projecte (on el servei encara el realitza el proveïdor sortint) per tal d'adquirir la dinàmica de l'operació del mateix.

Després del procés d'acompanyament, l'adjudicatari del present contracte assumirà la gestió del manteniment correctiu derivat del projecte **durant sis mesos sense cost per l'IMI**, comptant a partir de la data de l'acta d'entrega.

En aquest cas, un cop finalitzada la recepció del nou servei, l'adjudicatari gestionarà les activitats que siguin necessàries i tots els serveis de manteniment que conformen la gestió d'aplicacions informàtiques (AM) en els termes descrits en el present plec de prescripcions tècniques.

El licitador haurà de presentar una proposta de diagrama de flux del procés de recepció i acompanyament de nous projectes. Es valorarà la claredat del diagrama plantejat i que els procediments siguin el més complets possibles i aplicables en un entorn com el del l'IMI, incloent la definició de la metodologia específica per al disseny de proves prèvies d'UAT.

3.2.6. Millores funcionals i parametrització

Aquestes tasques refereixen habitualment a aquesta tipologia d'activitats de modificació i creació:

- Canvis en informes (afegir, modificar/eliminar camps i filtres)
- Canvis en models de càlcul
- Canvis en pantalles ja existents (afegir/modificar/treure) camps, afegir/canviar validacions en processos
- Canvis en els fluxos de funcionament i operació del sistema (afegir/modificar/treure) passos
- Canvis en els processos batch i la seva planificació analitzant totes les altres cadenes actives i les finestres disponibles
- Canvis i adaptacions en els processos i serveis d'integració amb tercers
- Canvis en la parametrització i configuracions dels sistemes
- Canvis en plantilles i documents
- Canvis en els processos d'extracció i/o publicació d'informació dels sistemes de gestió cap a altres sistemes (Business Intelligence, Data Warehouse, Open Data, eArxiu, etc.). Realitzar peticions concretes d'extracció.
- Nous o canvis rols d'autoritzacions motivats per canvis organitzatius
- Acompanyament funcional o tècnic de més de 3 jornades
- Altres de característiques similars

3.2.7. Formació

S'inclouen tasques relacionades amb formacions tècniques o funcionals. Aquestes formacions poden ser presencials i/o realitzades en la plataforma de formació que l'IMI determini, de manera que quedin preparades per a utilitzar-se en el futur.



Inclou les tasques associades a la preparació, impartició i avaluació de la formació. A criteri de l'IMI es durà a terme una, vàries o totes aquestes fases per cada formació concreta.

Es fomentarà en tot cas la impartició de formació online que permeti l'autoconsum o la publicació periòdica dins de la plataforma de formació que l'IMI determini.

De la mateixa manera podria ser requerit per circumstàncies concretes la formació específica i presencial o en remot en centres de l'Ajuntament de Barcelona.

En cas de requerir trobades presencials, els viatges i dietes dels participants de l'adjudicatari o les seves empreses subcontractades seran a cost de l'adjudicatari, sense cap cost addicional per l'Ajuntament de Barcelona. En aquests casos l'Ajuntament ho comunicarà via correu electrònic almenys amb una setmana d'antelació per facilitar la organització dels viatges, si s'escau.

Serà responsabilitat de l'adjudicatari la preparació i actualització constant dels entorns de formació, jocs de proves i la realització de proves i certificació de l'entorn de proves previ a la formació en cas de ser necessari. L'actualització permanent dels entorns de formació, és crítica, ja que s'utilitzen per formar a nous usuaris de manera continuada. Es requereix que l'entorn de formació estigui sempre igualat a l'entorn productiu.

És responsabilitat de l'adjudicatari la realització d'enquestes de valoració en cada sessió de formació realitzada, les quals tindran caràcter obligatori. L'IMI transmetrà les necessitats de l'enquesta i l'adjudicatari realitzarà una proposta de contingut alineada a les necessitats transmeses per l'IMI. Serà necessària la validació del contingut per part de l'IMI, qui determinarà el contingut i format final de l'enquesta.

L'adjudicatari haurà d'utilitzar l'eina d'enquestes per a la preparació i enviament de les enquestes, i presentarà el resultat de les enquestes de cada sessió de formació a l'IMI. Les puntuacions de cada pregunta de l'enquesta podran ser de 0 (mínima valoració – gens satisfet) fins a 5 (màxima valoració – molt satisfet). A l'eina s'identificaran les persones que entren a realitzar cada enquesta.

En el cas que la mitjana global de totes les enquestes d'una formació sigui inferior a 2,5 (sobre 5), l'adjudicatari haurà de repetir la formació sense cost addicional per l'IMI, resolent el que sigui necessari per resoldre les incidències identificades (canvi de consultor, canvi de joc de dades,...).

De la mateixa manera, en cas que la documentació o entorn preparat per dur a terme la formació manifesti mancances de qualitat o omissions no identificades per l'adjudicatari, la revisió i correcció de les mateixes correrà a càrrec de l'adjudicatari.

En cas de rotació de l'equip de treball de l'adjudicatari la nova incorporació ha de ser formada i preparada convenientment. En aquest sentit hi ha diferents tasques que ha de dur a terme el proveïdor i que no han de tenir repercussió a l'IMI. En aquests casos aquestes tasques hauran de ser imputades al JIRA dins d'aquest subservei i amb Garantia = "Sí" per tal



que no computin a l'hora de realitzar la facturació mensual. Tant la nova incorporació com el personal que li doni suport haurà d'imputar aquí les hores dedicades al respecte:

- Gestió d'alta i permisos
- Preparació i configuració dels entorns de treball.
- Formació i documentació
- Shadowing o paral·lel amb la persona sortint en cas de ser necessari. Aquest últim concepte només a imputar per persona entrant.

3.2.8. Sondes de monitorització i consultes preventives

L'adjudicatari és responsable de dissenyar i implantar sondes de monitorització pels nous casos d'ús que s'incorporin durant l'execució del contracte i pels casos d'ús prèviament existents que no disposin de sonda i que l'IMI consideri que la necessiten.

L'adjudicatari haurà de realitzar una anàlisi de les sondes existents i la seva adequació, i identificar les sondes que requereixen evolució i les noves sondes que es necessitarien implantar.

Serà responsabilitat de l'adjudicatari la realització de les següents tasques:

1. Creació del disseny d'un test de navegació per validar les principals funcionalitats de les aplicacions, tenint en compte les consideracions i procediment descrits a continuació.
 - La navegació ha de simular l'ús de les aplicacions per part de l'usuari de l'Ajuntament de Barcelona i del ciutadà. L'Ajuntament proporcionarà estadístiques de les pàgines més visitades per tal que l'adjudicatari pugui dissenyar una navegació representativa.
 - La navegació ha de validar el màxim de mòduls de l'aplicació i d'integracions amb altres sistemes prioritzant les funcionalitats que impactin directament al ciutadà.
 - Les validacions de les integracions no han d'impactar als altres sistemes ni crear registres inconsistents, però no ha de ser aquesta la raó per no programar aquestes validacions. La solució serà contemplar a l'inici del desenvolupament una opció de navegació pels robots Nimbus que no impacti als sistemes integrats amb una no resposta acceptada per l'aplicació que permeti continuar els passos habituals de l'usuari final.
 - Si és necessari s'haurà de contemplar des del desenvolupament de l'aplicació la creació i manteniment de jocs de dades a les BBDD de Producció per utilitzar-les com a casos reals a les navegacions que es programin pels tests Nimbus (p.ex.: dades de padró, dades de tributs, dades itineraris, etc.).
 - S'ha d'obrir petició de creació nova sonda a través de l'eina estàndard de l'IMI, omplint la plantilla de petició i adjuntat la documentació del disseny.
 - També s'haurà de donar suport a l'equip tècnic de Gestió de la Disponibilitat fins la distribució a producció de la programació de la sonda, i si és necessari per requeriments tècnics modificar el disseny de la sonda.



2. Manteniment i revisió del disseny del test de navegació.

- Actualitzar el disseny quan es doni alguna d'aquestes situacions i tenint en compte el procediment indicat a continuació:
 - En cas d'actualització de l'aplicació: si es modifiquen els menús, pantalles i/o funcionalitats que utilitza cada sonda.
 - En cas d'actualització del client pesat, s'ha de revisar la sonda i si cal sol·licitar les modificacions necessàries a la navegació.
 - En altres casos de millora o optimització de la navegació.
- Per incloure noves validacions al test de navegació:
 - S'ha d'obrir petició de modificació de sonda a través de l'eina estàndard de l'IMI, adjuntant la documentació del disseny modificat. També s'haurà de donar suport a l'equip tècnic de Gestió de la disponibilitat dins la distribució a producció de la programació de la sonda, i si és necessari per requeriments tècnics modificar el disseny de la sonda.

Canvis al programari: En general les sondes han d'executar-se amb la mateixa lògica que implementa els casos oferts a l'usuari i en ocasions requeriran la construcció del cas de test o modificacions en el comportament en el cas d'ús existent per l'usuari, utilitzats pel test Nimbus. Per exemple: no escriure determinat registre o esborrar dades creades durant el test. En aquests casos pot ser necessari incorporar línies de codi exclusives pel test. Aquests canvis al programari orientats a la creació de tests es consideren part del manteniment recurrent.

Un tipus especial de sondes relacionades amb dades de negoci són les **consultes preventives**, les quals permeten assegurar la coherència i qualitat de les dades. L'adjudicatari serà responsable de dissenyar-les i implementar-les. Es monitoritzaran setmanalment fent reporting del seu resultat i en cas de detectar alguna inconsistència interna en les dades de negoci es realitzaran les tasques necessàries per a resoldre la incidència, amb el suport de l'usuari referent si fos necessari.

S'inclouen també en aquest subservei les tasques necessàries per a validar les execucions dels processos batch en cas de no cancel·lació, i així disposar d'eines per validar el seu correcte funcionament.

3.2.9. Transició

L'objecte del subservei de transició és assegurar que el traspàs d'informació entre adjudicataris **a l'inici i a la finalització del contracte**, es realitza correctament, sota els estàndards de qualitat exigibles i assegurant el traspàs d'informació i de coneixement. Tanmateix, s'ha de garantir la continuïtat dels serveis prestats en els termes que s'especifiquen en el present plec.

La transició es realitzarà de manera particular per cada servei-aplicació que compongui el contracte. D'aquesta manera, les diferents durades de la transició s'hauran d'ajustar per tal que totes les transicions a realitzar finalitzin a temps per iniciar la prestació del serveis a la data requerida.



La transició (recepció o devolució) de cada servei-aplicació únicament es farà efectiva quan l'adjudicatari sortint i el nou adjudicatari siguin proveïdors diferents. Quan hi hagi continuïtat de proveïdor, aquesta tasca no caldrà executar-la.

S'entén que hi ha continuïtat de proveïdor davant els següents supòsits:

- És el mateix proveïdor el sortint que l'entrant
- El proveïdor entrant forma/va part de la UTE del proveïdor sortint
- El proveïdor sortint forma/va part de la UTE del proveïdor entrant
- El proveïdor sortint és subcontractat pel proveïdor entrant
- El proveïdor entrant i el sortint formen part del mateix grup empresarial

En el cas particular que algun dels proveïdors adjudicataris entrants hagi format part de l'UTE adjudicatària sortint, però fos necessari realitzar la transició d'algun servei-aplicació, aquesta es realitzarà a càrrec de l'adjudicatari i sense cost addicional per l'IMI.

L'IMI determinarà les tasques de transició necessàries per garantir el correcte traspàs del coneixement i es gestionarà com un manteniment recurrent. L'adjudicatari haurà de realitzar les accions definides al Pla de Recepció/Devolució del servei acordat i validat per IMI.

S'estimen les següents fases en la Transició:

- Reunions i documentació:
 - Planificació i realització de reunions funcionals i tècniques amb adjudicatari sortint i quan sigui necessari amb IMI i usuari final.
 - Recepció i estudi de la documentació de traspàs.
- Test de shadowing: Si l'IMI ho considera necessari, l'adjudicatari entrant/sortint durant el període de transició pot arribar a dur a terme dins del present subservei, una tasca de shadowing o paral·lel en funció del servei-aplicació:
 - Tests en entorn pre-productiu
 - Tests en entorn productiu
- Finalització Transició:
 - Lliurament informe finalització transició.

S'estima que, per realitzar el procés de recepció/devolució de cada servei, caldrà una dedicació aproximada del **50%** de l'equip estimat per a la prestació dels serveis objecte del contracte.

En el cas del traspàs d'informació entre adjudicataris a l'inici (recepció) del contracte -cada un dels serveis/aplicació presenta els mesos de transició requerits i l'import assignat per a la seva realització (veure informació de detall al document Excel adjunt "**Càlcul detallat import de contracte_AM HOSTLAMP, Càlcul pressupost, columnes U i V**"). La transició es gestionarà com un subservei de manteniment recurrent en el cas que apliqui realitzar-la. S'haurà de complir el següent flux de tramitació:

- L'IMI utilitza l'import determinat a la documentació de la licitació (Excel de càlcul), per a la recepció de cada servei-aplicació com a valoració acceptada.



- L'adjudicatari presentarà a l'IMI, en la reunió de KickOff, el pla de treball, que haurà d'incloure com a mínim:
 - o El detall de les tasques a realitzar en la Transició.
 - o La planificació del servei de transició, assegurant la coordinació de les transicions específiques en fases, per a cada servei d'aplicació i els procediments proposats que permetin l'assegurament de la continuïtat del servei i del traspàs de la informació.
 - o La proposta de l'organització dels recursos i equip involucrats en el servei de transició.
- L'adjudicatari imputarà les hores realitzades per cadascun dels seus treballadors en l'eina de gestió de ticketing de l'IMI.
- En acabar la transició l'adjudicatari presentarà a l'IMI l'informe de finalització de la transició amb el pla de treball i el detall de les tasques realitzades.

Test de shadowing

Per tal d'assegurar el compliment del procés de recepció del servei tal i com es defineix en el present plec de prescripcions tècniques, l'IMI podrà exigir, a la meitat del temps estipulat per a la transició, la realització d'un test per a comprovar l'avenç de la transició per a aquells serveis més complexos, de manera que es comprovi el nivell de coneixement adquirit per part del receptor del servei.

El test de shadowing el realitzarà l'adjudicatari i serà supervisat pel proveïdor sortint.

Aquesta prova o test podrà constar de tasques en entorn pre-productiu i tasques en entorn productiu.

Per l'entorn productiu, al considerar-se part de la Transició, les tasques estaran supervisades per l'adjudicatari sortint: Resolució d' incidències reals i realització de manteniments recurrents reals i es realitzaran en entorn pre productiu i una vegada validat es transportarà a l'entorn productiu.

Aquesta prova serà definida per l'IMI, en base a les característiques i necessitats (contingut i durada de la prova), i serà comunicada a l'adjudicatari amb un mínim d'un mes de la seva execució.

Un cop finalitzat el test, l'IMI determinarà si el receptor del servei ha superat de manera satisfactòria el test o si, per contra, el resultat ha sigut insatisfactori.

- Si el resultat ha sigut satisfactori, la transició s'haurà de completar tal i com s'hagi estipulat en el present plec de prescripcions tècniques.
- Si el resultat ha sigut insatisfactori:
 - o Haurà de repetir el test una setmana després. Si per segon cop consecutiu el receptor del servei no ha superat satisfactòriament el test, s'escalarà a la Direcció de l'IMI la situació perquè prengui les mesures necessàries, entre les quals poden resultar:



- Es penalitzarà econòmicament al receptor del servei amb una rebaixa del 50% del preu de la factura de la fase transició
- Es considerarà una falta greu

3.2.9.1 Tasques rellevants de recepció del servei

A efectes il·lustratius, es detallen algunes de les tasques més rellevants a dur a terme durant la recepció del servei, sota l'objectiu principal de donar continuïtat al servei dels prop de 1050 desplegaments web **sense cap mena de tall de servei al ciutadà**:

- Formalitzar i organitzar l'equip de treball dedicat al projecte
- Transferència de coneixement al nou adjudicatari
 - Recepció de la documentació tècnica de la infraestructura
 - Recepció de la llista definitiva de webs i la localització dels desplegaments
 - Recepció de la documentació d'estàndards de programació Python/Django
- Recepció de la infraestructura
 - Recepció de les claus d'administració i la informació de detall necessària per gestionar el traspàs de la subcontractació del IaaS, monitorització i còpies de seguretat actual.
 - Canviar la configuració de pagament de la subcontractació del IaaS, monitorització i còpies de seguretat actual, per assumir completament el seu cost per part del nou adjudicatari
 - En cas de que l'adjudicatari consideri la migració a un nou proveïdor de hosting, es podrà fer un cop assumit el servei, i en tot moment assegurant els acords de nivell de servei, i que per tant no hi ha afectació cara als usuaris finals de la plataforma.
- Recepció dels webs i aplicatius
 - Transferència de coneixement de la gestió de serveis en curs o previstos en aquest contracte, mitjançant sessions planificades entre l'IMI i l'adjudicatari.
 - Traspàs de la responsabilitat de mantenir els webs i la infraestructura
 - Inici de l'aplicació dels acords de nivell de servei de suport.

Els licitadors han de presentar una proposta de Pla de Recepció del Servei en el conjunt de documentació tècnica (veure apartat **10.1 Proposta tècnica: Sobre B: Recepció infraestructura**) , amb el detall suficient que permeti la valoració de la seva viabilitat, coherència, realisme, estructura organitzativa.



3.2.9.2 Possibilitat de Trasl·lat dels servidors actuals a un nou proveïdor

L'adjudicatari pot considerar el moure la infraestructura cap a un nou allotjament que compleixi com a mínim totes les especificacions del servei actual, sense cap cost afegit per l'IMI, i garantint en tot moment la disponibilitat del servei i el compliment de tots els requeriments especificats.

No es limita l'àmbit geogràfic del trasllat, tot i que, en cas de fer el trasllat, haurà de ser prèvia aprovació de l'IMI, i un cop recepcionat el servei per part de l'adjudicatari.

En tot cas s'haurà d'assumir el servei actual, independentment de si a curt termini es trasllada a un altre allotjament.

El proveïdor de hosting ha de complir:

- Els estàndards expressats a la norma sobre seguretat: ISO 17799:2005, ISO 27001 (Gestió de la Seguretat de la Informació per a la provisió de Serveis Professionals de Cloud, Hosting i Housing), i OWASP, ENS segons el RD 311/2022 de 3 de maig (nivell Bàsic), i els que siguin d'aplicació o l'IMI indiqui durant l'execució del contracte.
- el que s'indica a l'introducció de l'apartat 11: "condicions generals"

Els licitadors han de presentar una proposta de **Infraestructura Destí** en el conjunt de documentació tècnica (veure apartat **10.1 Proposta tècnica: Sobre B: Infraestructura Destí**), amb el detall suficient que permeti la valoració de la seva viabilitat, coherència, i la justificació del seu benefici.

3.3. Desenvolupament d'evolutius identificats

Els serveis d'evolutius són aquells que s'executen a petició de l'IMI i que estan identificats en el moment de redacció d'aquest Plec de Prescripcions Tècniques (veure a l'Annex 5: apartat 17.2 el flux actual de evolutius identificats a l'eina de ticketing).

Són modificacions i millores orientades a actualitzar/ampliar les funcionalitats actuals dels sistemes d'informació amb l'objectiu de donar resposta a les peticions i requeriments dels usuaris d'aquests sistemes.

L'objectiu d'aquesta activitat és la realització de les tasques necessàries per continuar amb la incorporació de noves funcionalitats per tal d'adaptar-ne l'objectiu global de l'aplicació a nous requeriments o bé adaptar-ne els existents.

En el present contracte no s'inclouen evolutius identificats.



3.4. Serveis d'evolutius recurrents

El servei d'evolutius recurrents fa referència a les tasques periòdiques relacionades amb canvis en els sistemes i processos, que resulten en millores dels diferents productes/actius.

El volum d'aquests serveis s'ha calculat tenint en compte l'històric. El detall de les volumetries s'especifica en l'Annex 2: Volumetries del present plec.

El seu increment o decrement pot ser motiu d'ampliació o de disminució del contracte segons allò previst a l'apartat de possibles modificacions del contracte per causes precises o previstes del plec de clàusules administratives particulars.

Tots els serveis d'evolutius recurrents atesos per aquest servei, en el transcurs del desenvolupament del contracte, hauran de complir el següent flux de tramitació:

- L'IMI comunica a l'adjudicatari l'evolutiu recurrent a realitzar i la seva prioritat.
- L'adjudicatari realitza una anàlisi tècnica prèvia del l'evolutiu recurrent i comunica a l'IMI, en el format que l'IMI determini, la informació de la valoració, l'esforç necessari i la data de lliurament en què es compromet a lliurar el recurrent a l'IMI. Les hores de valoració s'imputaran en el tiquet de l'eina.
- Per a tots els serveis d'evolutius recurrents, en cas que l'evolutiu recurrent al final no es realitzi i només s'hagi valorat, el tiquet amb les seves imputacions d'hores es cancel·larà i es modificarà com a servei de contracte de Serveis Transversals de Manteniment (STM), tasca de suport tècnic.
- L'IMI analitzarà la valoració i la data presentada pel proveïdor:
 - o **L'adjudicatari no podrà imputar hores fins que la tasca no hagi estat acceptada per l'IMI (excepte les necessàries per a la valoració)**
 - o En el cas d'estar d'acord podrà donar aprovació a l'inici dels treballs.
 - o En cas d'identificar alguna necessitat d'aclariment, s'iterarà amb l'adjudicatari fins resoldre'l.
 - o En cas que la valoració i estudi previ realitzats manifestin mancances de qualitat o faltant no identificats correctament per l'adjudicatari, la revisió i correcció de les mateixes correrà a càrrec de l'adjudicatari en concepte de garantia i sense cost per a l'IMI, a banda de l'aplicació del corresponent ANS.
 - o La data d'entrega planificada proposada per l'adjudicatari haurà de tenir present tots els serveis inclosos al recurrent i les seves respectives dates intermèdies. L'adjudicatari la presentarà i explicarà a l'IMI per obtenir la seva validació.
 - o La coordinació amb tots els agents implicats en cada recurrent serà responsabilitat de l'adjudicatari.
 - o En cas de no ser acceptada per l'IMI, tant per valoració (estimació d'esforços necessaris), com per planificació, el proveïdor estarà obligat a presentar una nova valoració/planificació, i estarà subjecte a l'ANS "Anàlisi i planificació de peticions (Plani)" (veure apartat de Serveis de Manteniment Recurrent).
 - o El procés d'aprovació serà conjunt IMI-proveïdor, on es fixarà la data de lliurament. Si un cop aprovada la data de lliurament hi hagués un canvi de



prioritat que afecta un evolutiu recurrent, l'IMI, d'acord amb el proveïdor, podrà replanificar la data de lliurament de l'evolutiu recurrent afectat.

- De la mateixa manera si s'identifica un canvi d'abast en l'evolutiu recurrent no imputable a l'adjudicatari, l'IMI, d'acord amb el proveïdor, podrà demanar la revaloració i replanificació de la tasca.

L'IMI es reserva el dret de contrastar les valoracions realitzades per altres mitjans. En concret i en el que es refereix a tasques tècniques o d'arquitectura l'IMI compta amb una àrea que se n'ocupa de les qüestions comuns i de suport transversal als desenvolupaments. En cas de conflicte o discrepància en l'enfoc de solucions o en l'estimació dels esforços a dur a terme, el responsable del contracte per part de l'IMI, arbitrarà i en cas de no resoldre's prevaldrà la solució i l'estimació realitzada per l'àrea d'arquitectura de l'IMI. En cas que sigui necessari l'IMI podria aplicar el descrit en l'apartat 7.3 Auditories, fins i tot aplicant el règim de faltes i sancions en funció del resultat de les mateixes.

El servei d'evolutius recurrents inclou aquests subserveis:

- Evolutius motivats per canvis normatius
- Evolutius motivats per actualitzacions tecnològiques
- Evolutius motivats per qualitat tècnica
- Evolutius motivats per millores funcionals i parametrització

És responsabilitat de l'adjudicatari complimentar a l'eina de ticketing de forma detallada tant la valoració de cada evolutiu recurrent (adicionalment a l'esforç total, es requereix el detall de les tasques principals i el seu esforç), com la informació de l'evolutiu recurrent (origen de la necessitat, anàlisi realitzat, valoració detallada, la seva resolució i tots els **documents generats**). També cal incloure detall a les imputacions realitzades. L'incompliment d'aquesta responsabilitat impedirà el tancament i la facturació del tiquet corresponent fins a la seva subsanació.

A continuació es detallen les tasques a realitzar en cadascun dels subserveis definits. En tots els casos, si el seu volum i complexitat ho requereix, o a petició de l'IMI, es gestionaran seguint la metodologia ADINET o Metodologia Agile, descrites als Annexes 3 i 4. D'aquesta manera s'assegurarà la definició de les tasques necessàries fins a la seva posada en producció: anàlisi de requeriments, disseny funcional, disseny tècnic i arquitectura d'aplicacions, desenvolupament, proves, proves d'usuari (si s'escau), implantació, i suport post-implantació.

3.4.1. Evolutius motivats per canvis normatius

Fan referència a aquells evolutius recurrents i les seves tasques necessàries per poder garantir que els sistemes s'adaptin a la legalitat vigent en cada moment, resultant per tant en un canvi en el producte o actiu.

L'adjudicatari està obligat a assumir la realització de tots els treballs necessaris per adaptar els sistemes d'informació objecte del contracte als canvis legals als quals es vegin afectats durant la durada del mateix.



3.4.2. Evolutius motivats per actualitzacions tecnològiques

Són les modificacions motivades per actualitzacions a l'entorn en què el sistema opera i que es fan per evitar l'obsolescència tecnològica i el manteniment actualitzat del programari.

Es consideren actualitzacions tecnològiques per exemple, els canvis de configuració del maquinari, el programari base, els gestors de base de dades, comunicacions, etc.

Un exemple d'actualització tecnològica són les actualitzacions de les versions de les aplicacions que es facin servir, adaptació de codi a les versions de php actuals...

És obligació de l'adjudicatari la realització de les actualitzacions tecnològiques de les aplicacions del contracte a les últimes versions dels productes base que s'utilitzen com a components, com poden ser els entorns de gestors de base de dades, servidors d'aplicacions, servidors web, navegadors, gestor documental, etc.

3.4.3. Evolutius motivats per qualitat tècnica

Són grans modificacions motivades per implementacions incomplertes o incorrectes dels sistemes o de les integracions amb tercers, tant a nivell tècnic com de funcionalitats requerides pels usuaris.

Normalment la seva existència suposa una càrrega en tasques de manteniment repetitives i improductives per tal de cobrir aquestes mancances.

Exemples de dèficit de qualitat tècnica són l'evolució del manual de tasques o processos automàtics i l'adaptació necessària dels mateixos en els sistemes, o la necessitat d'evolució de les funcionalitats d'administració per part de l'usuari en la gestió autònoma del sistema.

En la mateixa línia, un dels objectius d'aquest contracte és la reducció del nombre d'incidències històriques que es produeixen en els sistemes, és per això que s'inclouen dèficit de qualitat tècnica l'evolució i millora dels sistemes via tasques de manteniment preventiu i perfectiu que han de permetre a l'adjudicatari la reducció del cost de manteniment futur:

- Manteniment preventiu. Modifiquen les aplicacions per millorar les seves propietats i facilitar el manteniment futur de les mateixes
- Manteniment perfectiu. Milloren el programari de les aplicacions en qüestions com rendiment, flexibilitat, reusabilitat, etc. L'objectiu d'aquestes millores és reduir el volum d'incidències, millorar el rendiment i facilitar l'ús i les integracions amb altres sistemes

La realització d'aquests evolutius recurrents es planificarà i es prioritzarà d'acord amb el responsable de servei en base a les necessitats del servei. És responsabilitat de l'adjudicatari identificar i proposar la correcció dels casos més destacats i recurrents dins de la prestació del servei.

3.4.4. Evolutius motivats per millores funcionals i parametrització



Aquestes evolucions recurrents inclouen habitualment aquesta tipologia d'activitats relacionades amb canvis en els sistemes i processos, que resulten en millores dels diferents productes/actius:

- Evolució dels informes del sistema
- Evolució dels models de càlcul
- Evolució de les pantalles ja existents i els seus elements principals, com poden ser la gestió de camps i de validació de processos
- Evolució dels fluxos de funcionament i operació del sistema
- Evolució de la parametrització i configuració dels sistemes així com de les eines de migració i ingesta massiva a l'eArxiu.
- Evolució de les plantilles i documents
- Evolució dels processos batch o serveis d'integració amb tercers.
- Evolució dels processos d'extracció i/o publicació d'informació dels sistemes de gestió cap a altres sistemes (Business Intelligence, Data Warehouse, Open Data, ...).
- Evolució dels rols d'autoritzacions motivats per canvis organitzatius

El licitador haurà de presentar una proposta de metodologia de desenvolupament per evolucions recurrents aplicable que els procediments siguin el més àgils i complets possibles, i aplicables en un entorn com el de l'IMI.

3.5. Serveis Transversals de Manteniment (STM)

Els Serveis Transversals de Manteniment (STM) tenen com a objectiu l'assegurament de la qualitat, la documentació, el govern i, en general, el correcte desenvolupament del contracte (veure a l'apartat 17.3, el flux actual a l'eina de ticketing).

Les tasques a realitzar pels Serveis Transversals de Manteniment estan estructurades en els següents grups:

- Operació:
 - Serveis de coordinació tècnica i funcional
 - Planificació, seguiment i control del servei
 - Assegurament de la qualitat
 - Coordinació incidències i problemes
 - Supervisió de sondes de monitorització i consultes preventives
 - Supervisió, planificació i reporting de processos batch
 - Administració de sistemes
- Suport:
 - Help Desk
 - Suport funcional
 - Suport tècnic
 - Coordinació de la documentació
- Gestió del canvi
 - Comunicació



- Coordinació de la transició del servei
- Gestió del contracte:
 - Reporting
 - Indicadors del Servei
 - Gestió de riscos
- Llicències i productes

Es diferencia entre tasques periòdiques que ha de realitzar el proveïdor i peticions o tasques puntuals que demana l'IMI o l'usuari, per exemple, suport funcional, suport tècnic, petició d'informació, aquestes darreres seran classificades com a màxima prioritat i estaran subjectes a ANS específics (veure apartat 8, ANS "Temps de resolució de petició (Pet Treso)". És responsabilitat de l'adjudicatari complimentar a l'eina de ticketing de forma específica el detall de les tasques realitzades en cada imputació. La manca de qualitat en el detall del tiquet i de les imputacions derivarà en la corresponent aplicació dels ANS associats.

Els licitadors hauran de presentar la seva proposta d'enfocament del Servei Transversal de Manteniment (STM), en concret per el que fa a la coordinació, assegurement de la qualitat, suport, reporting i la transició del servei (veure apartat dels criteris d'adjudicació).

3.5.1. Operació

3.5.1.1 Serveis de coordinació tècnica i funcional

Els Serveis Transversals de Manteniment han de garantir la totalitat de les integracions amb la resta de sistemes d'informació i les seves corresponents infraestructures i arquitectures, així com coordinar totes les actuacions sobre les aplicacions dins del seu abast, amb la resta d'interlocutors, per tal de garantir la correcta execució de les diferents accions a dur a terme.

Per tal d'assegurar aquest servei l'adjudicatari haurà de realitzar les següents tasques:

- Tenir una visió a nivell de gestió global de les dependències existents entre tots els stakeholders involucrats
- Vetllar per l'alineament entre tots ells
- Coordinar amb els diferents stakeholders existents per a la realització de manteniments, integracions i proves
- Controlar, assegurar i garantir la coherència de les diferents accions realitzades durant l'execució del servei.
- Actuar proactivament en la supervisió del funcionament i en el seguiment dels possibles problemes i incidències relatives a les integracions, infraestructures, arquitectures i sistemes de les quals depenen els serveis de l'àrea, malgrat que el diagnòstic indiqui que no és responsabilitat directa del propi manteniment: seguiment estat, proves conjuntes, comunicació, accions de contingència. L'empresa



adjudicatària haurà d'elaborar un quadre de comandament global del servei amb la totalitat d'indicadors tècnics i de negoci necessaris per presentar el funcionament del servei i les seves aplicacions, mostrant la volumetria dels principals indicadors de negoci del mes anterior i presentant de manera visual les anomalies detectades i un breu anàlisi de les mateixes. Aquest quadre de comandament global del servei s'inclourà en els comitès de direcció.

- Informar, de forma proactiva i en tot moment, al responsable del contracte de possibles problemes, mal funcionaments o millores d'aquesta coordinació i dels serveis que en depenen.
- Donar resposta a les peticions de l'IMI a nivell de reporting, documentació i/o dades relacionades amb el servei.

En cap cas pot ser repercutible a l'IMI l'excés de gestió derivat de l'organització interna en cas de subcontractació, formació i gestió d'Unions Temporals d'Empreses, o fins i tot de les ineficiències causades per la pròpia organització interna d'equips plantejada per l'adjudicatari per la prestació del servei. L'IMI vetllarà perquè així sigui i s'eliminaran aquestes imputacions en cas de detectar-se.

3.5.1.2 Planificació, seguiment i control del servei

S'inclouen les activitats de control, coordinació i seguiment de tots els serveis de contracte inclosos en l'abast: serveis de manteniment correctiu, manteniments recurrents, evolutius identificats, evolutius recurrents, Serveis Transversals de Manteniment (STM) i aprovisionament de la infraestructura.

En el cas dels serveis de manteniments correctius i recurrents, els Serveis Transversals de Manteniment tindran les següents responsabilitats:

- Interlocució única amb el responsable del servei per part de l'IMI
- Estimacions d'alt nivell de les peticions rebudes
- Planificació de les peticions en base a una prioritització acordada prèviament amb l'IMI
- Gestió:
 - o Gestió i assignació de recursos
 - o Gestió de riscos i desviacions
 - o Gestió de problemes
- Control i seguiment:
 - o Control del servei
 - o Mesura i avaluació de la qualitat dels desenvolupaments en base als ANS del contracte
 - o El proveïdor generarà informes que permetin a l'IMI el seguiment de l'activitat dels serveis i definir estratègies de millora. Es concreten en l'apartat Reporting d'aquest plec.
- Assegurar l'observació dels estàndards tècnics:
 - o El proveïdor haurà de desenvolupar la seva activitat amb la més estricta observació de la metodologia de la documentació, desenvolupament o proves de traspàs a producció sota els estàndards de l'IMI, que són propis però a l'hora, similars als de qualsevol organització de la mateixa mida.



- Assegurar l'observació dels estàndards expressats a la norma sobre seguretat ISO 17799:2005, ISO 27001 i OWASP, ENS, i els que siguin d'aplicació o l'IMI indiqui durant l'execució del contracte.

En el cas dels serveis d'evolutius identificats i evolutius recurrents, els STM tindran les següents responsabilitats:

- Activitats de control i seguiment centrades en la monitorització de l'estat dels evolutius, la gestió de la resolució de problemes i la informació de l'estat al Comitè de seguiment del contracte. S'inclouen també els serveis de gestió i planificació de la implementació.
- Manteniment de la informació en l'eina de seguiment de projectes (veure apartat 6: Eines).

Aquestes activitats han de permetre corregir desviacions i detectar problemes inclús abans que aquests es presentin. Es realitzen mitjançant captura permanent d'informació de l'estat del contracte i la comparació de l'estat real amb el planificat, analitzant els indicadors de desviacions actuals o previstes.

L'IMI podrà plantejar una revisió de les previsions de la Línia Base dels serveis de negoci del contracte en base a prioritats i identificació de necessitats del propi IMI. Aquest tema es tractaria en Comitè de Direcció. L'adjudicatari haurà d'ajustar els equips i distribucions previstes el més aviat possible i en un període d'1 mes com a màxim.

3.5.1.3 Assegurament de la qualitat

El servei d'Assegurament de la Qualitat inclou el compliment de les metodologies que són d'aplicabilitat a l'entorn de l'IMI. Aquestes metodologies són ADINET o AGILE, segons apliqui. El contingut d'aquestes metodologies es recull als Annexes 3 i 4 del present document. En elles es defineixen un conjunt d'activitats i fases orientades a estructurar els processos de desenvolupament d'aplicatius. La seva correcta execució garanteix la generació d'un conjunt d'evidències associades a cadascun dels subprocessos que formen les metodologies (documentació, programari i proves) en les eines que l'IMI exigeix per a tal efecte (veure apartat 6: Eines). La gestió de la qualitat implicarà la monitorització d'aquestes evidències mitjançant punts de control anomenats checkpoints.

Tanmateix, el servei d'assegurament de la qualitat ha de garantir el compliment i adherència als requisits d'arquitectura establerts per l'IMI.

El Servei d'Assegurament inclou les següents activitats per cadascuna de les dues vessants de les quals es compona:

- 1. Assegurament del compliment de la metodologia ADINET – metodologia AGILE.** En els casos que apliqui l'ús d'aquesta metodologia, el proveïdor haurà de garantir que es porten a terme les següents validacions i verificacions:
 - Processos i procediments: Assegurar el compliment i adherència als processos i procediments establerts en ADINET – Metodologia AGILE.



- **Documentació:** validació de tota la documentació entregada a l'IMI, comprovant que s'adhereix completament a les plantilles i eines proporcionades per l'IMI en quant a format i contingut. Tots els documents hauran d'estar signats a la capçalera de control del document pel responsable assignat.
- **Programari:** Validació del programari d'acord als estàndards proporcionats per l'IMI.
- **Processos massius (batch):** Verificació i validació de l'execució de processos batch amb resultat final de no-cancel·lació.
- **Proves:** verificació i validació de tot el procés de proves, incloent la definició d'una estratègia de proves, l'execució dels diferents tipus de proves definides i el seu enregistrament.
- **Pla de qualitat:** assegurar el compliment i adherència definits en el pla de qualitat establert pels serveis descrits en el present plec, tal i com es desenvolupa a l'apartat 7.1 Pla de Qualitat.

2. Assegurament de l'adherència de les arquitectures plantejades. El proveïdor haurà de garantir que es porten a terme les següents validacions i verificacions des del punt de vista arquitectònic i de programari. Haurà de realitzar les activitats necessàries per garantir que les arquitectures proposades per cadascun dels nous desenvolupaments siguin conformes als estàndards i mòduls comuns IMI:

- **Arquitectura:** assegurament que les arquitectures plantejades per cadascun dels nous desenvolupaments i grans evolutius són conformes als estàndards i mòduls comuns de l'IMI, suportant totes les funcionalitats a realitzar.
- **Programari:** assegurament que els programaris es desenvolupen respectant l'arquitectura, estàndards i mòduls comuns de l'IMI.

Aquest servei ha d'estar garantit pels perfils únics, transversals i comuns a tots els serveis coberts pel contracte.

3.5.1.4 Coordinació incidències i problemes

Serà responsabilitat dels Serveis Transversals de Manteniment (STM) realitzar la comunicació a l'IMI i el posterior seguiment de les incidències i problemes més rellevants que es deriven de la posada en marxa i de l'execució dels diferents serveis dins del contracte.

Es considerarà problema aquella incidència o agrupació d'incidències que, amb el vistiplau previ de l'IMI, i per la seva reiteració o elevada necessitat de dedicació per a la seva resolució, es passi a gestionar de manera unificada i planificada tant pel que respecta a la seva resolució, com a la seva gestió a l'eina de ticketing. En aquest cas caldrà identificar les accions a fer per resoldre el problema i donar una data de resolució. La coordinació d'incidències i problemes pot requerir l'assistència a reunions i comitès.

Aquestes incidències i problemes més rellevants requeriran d'una supervisió més exhaustiva i un reporting amb una freqüència a determinar per l'IMI, informant del seu estat, les accions realitzades, les properes passis i l'impacte identificat. La resolució no podrà superar els **3 mesos** des de la seva aprovació com a tiquet problema.



Els STM hauran de tenir una visió transversal, per supervisar i coordinar, en cas que existeixin, les interdependències entre incidències i problemes de la mateixa o d'altres Direccions, així com potenciar i facilitar sinèrgies si n'hi haguessin. És per aquest motiu, que qualsevol incidència haurà de ser reportada a l'IMI a través dels STM.

Els STM hauran de saber en tot moment l'estat de les incidències i problemes reportats, i un cop estiguin resoltes, responsabilitzar-se de resposta per part de l'usuari per poder ser tancades de forma definitiva. Els STM informaran a l'àrea o àrees afectades de la resolució de les incidències, i en el cas que aquestes derivin en peticions de millora justificar-ne els motius als usuaris afectats.

3.5.1.5 Supervisió de sondes de monitorització i consultes preventives

L'adjudicatari serà responsable de supervisar l'execució diària, setmanal i mensual de les sondes de monitorització i en concret les alarmes generades en quant al seu mal funcionament. Aquestes alarmes generaran un tiquet d'incidència a tractar des de l'equip de manteniment correctiu. L'adjudicatari com a resposta a la incidència haurà d'estar alerta i actuar proactivament davant els problemes que es puguin ocasionar per dur a terme el seu diagnòstic, resolució i proposta de continuïtat dels processos afectats.

Es monitoritzaran setmanalment fent reporting del seu resultat i en cas de detectar alguna inconsistència interna en les dades de negoci (el contingut publicat al web) es realitzaran les tasques necessàries per a resoldre la incidència, amb el suport de l'usuari referent si fos necessari.

L'adjudicatari haurà de proposar, en base a l'operativa de les sondes, millores sobre les mateixes per afinar la detecció d'errors, evitar falsos positius i millorar la detecció de problemes crítics. De la mateixa manera haurà d'actuar proactivament per plantejar recurrents que permeten reduir les incidències o problemes derivats d'aquestes identificacions automàtiques.

Un altre tipus de sondes relacionades amb dades de negoci són les **consultes preventives**, les quals permeten assegurar la coherència i qualitat de les dades. L'adjudicatari serà responsable d'executar-les amb la periodicitat requerida.

És responsabilitat també de l'empresa adjudicatària la monitorització i supervisió continuada del bon funcionament de les aplicacions dels serveis i les tecnologies incloses a l'abast del contracte. Aquestes tasques són especialment necessàries en l'evolució tecnològica que s'està duent a terme actualment amb la nova arquitectura que utilitza kubernetes, ja que amb aquesta nova arquitectura l'empresa adjudicatària és responsable de:

- la gestió tècnica de l'aplicació,
- realitzar els desplegaments en la nova arquitectura,
- parametritzar la seva infraestructura,
- i detectar i resoldre anomalies en aquests elements.



L'empresa adjudicatària haurà d'elaborar mensualment i presentar en el Comitè de Direcció, un quadre d'indicadors tècnics per presentar la situació dels serveis per tecnologia i les propostes de millora de parametrització (destacant els serveis en tecnologia kubernetes).

3.5.1.6 Supervisió, planificació i reporting de processos batch

L'adjudicatari serà responsable de supervisar l'execució diària, setmanal, mensual o la freqüència que sigui necessària, dels processos batch, de reportar els seus resultats en un correu diari amb tot el detall, i gestionar les cancel·lacions quan es produeixin o les seves replanificacions quan el servei ho requereixi.

En cas d'aturada de servei per qualsevol motiu, l'adjudicatari és responsable de dissenyar les replanificacions dels processos batch, acordant amb l'Oficina Batch de l'IMI la replanificació i el nou calendari i fent la comunicació a l'usuari referent.

L'adjudicatari com a resposta a la incidència haurà d'estar alerta i actuar proactivament davant els problemes que es puguin ocasionar per dur a terme el seu diagnòstic, resolució i proposta de continuïtat dels processos afectats. En el cas de cancel·lació per problemes o inconsistència de dades, l'adjudicatari haurà de validar la correcció de les causes del problema/inconsistència abans de la següent execució.

En cas de processos batch executats amb resultat final de no-cancel·lació, és responsabilitat de l'adjudicatari la revisió de les dades actualitzades o generades per a la seva validació, informant del resultat en cas de disfunció.

3.5.1.7 Administració de sistemes

Aquestes tasques s'agrupen en:

- **Administració del programari base (PaaS):** Prestar el servei de suport tècnic i administració dels servidors, duent a terme tasques de configuració, millora del rendiment, canvis necessaris per la incorporació de nous webs i interlocució amb el servei d'infraestructura i còpia de seguretat.
- **Administració de webs CMS i aplicatius LAMP:** Assegurar que el rendiment dels webs és bo, aplicant mesures d'optimització, revisant la qualitat de les mateixes, Mantenir una guia de bones pràctiques de desplegament, Donar suport a problemes de funcionament o de rendiment a la plataforma, potenciar eines autonomia desenvolupadors.

A continuació es detallen les tasques habituals d'administració:

(Serveis d'Administració de Sistemes): Administració del programari base (PaaS)

En concret, relacionat amb els webs CMS, es poden donar habitualment alguns dels següents aspectes que requereixen un servei d'administració immediat:

- Problemes de rendiment dels webs, que afecten els recursos del clúster



- Caigudes d'un web concret, a causa d'una punta de visites, d'una falla de programació, o d'una saturació momentània a causa d'una actualització de memòria cau massiva
- Ajustos urgents de configuracions de sistema per permetre el funcionament d'un web CMS amb requeriments específics no detectats prèviament.
- Configuracions dels CMS per ajustar un web que pot està perjudicant la infraestructura en quant a càrrega i rendiment, per exemple en el cas de tenir la memòria cau Drupal desactivada, tenir els fitxers de traces de Debug activats a producció, falta de configuració de la memòria cau Redis o alt tràfic de base de dades degut a insercions massives.
- Actuacions per recuperar un web, incloent diagnòstic i si s'escau, en cas de no poder contactar amb el programador , modificar directament el web per donar continuïtat al servei.
- Posar en quarantena un web si es sospita que la seva seguretat ha estat compromesa.
- Recuperació urgent d'una còpia de seguretat, ja sigui de codi, contingut, o de base de dades. O bé recuperació de configuració de configuració que estigui afectant negativament el servei.
- Aplicació urgent de pegats de seguretat crítics (respectant els acords mínims establerts a l'apartat 8.1.6 : "aplicació de pegats del sistema").

Funcions principals

A continuació es descriuen els requisits mínims a complir per cobrir el servei de suport tècnic. Concretament, les funcions a cobrir són:

- Creació de nous entorns en el servei de cloud: serà l'encarregat de desplegar nous entorns a l'entorn cloud, a demanda del client o de la necessitat de creixement. Això inclou també, si s'escau, la configuració del sistema base, instal·lació de paquets i serveis, configuració d'aquests, i generació d'imatges de les màquines finalistes. Aquestes tasques s'han de dur a terme sempre que sigui possible via IaaS (saltstack) i no directament a la infraestructura, i en tot cas deixar sempre documentats els canvis.
- Gestionar les infraestructures, cercant vulnerabilitats i proposant millores sobre aquestes.
- Gestió dinàmica del firewall, tant per la configuració inicial, com per canviar-lo dinàmicament segons requeriments (per exemple, per bloquejar el tràfic sortint d'un servidor si aquest ha quedat compromès).
- Interfície amb el servei de cloud: totes les incidències amb el servei de cloud hauran de ser gestionades per l'adjudicatari fins a la seva resolució.
- Els serveis/tecnologies mínims a gestionar sobre la infraestructura es detallen a l'apartat "4.5.1: Entorn públic AWS".

En concret, formant part de l'operativa del dia a dia, es duran a terme les següents tasques:



Manteniment del programari base

- Manteniment de la configuració de màquines virtuals (frontal i base de dades) (via SaltStack), per tal que estiguin al dia en quant a seguretat i versions de programari usades.
- Administració dels servidors: aplicar actualitzacions del sistema, verificar el bon funcionament de: monitors nagios, còpies de seguretat, espai disponible de disc, no saturació de CPU/RAM, antivirus.
- Revisió seguretat del programari base.
- Donat l'alt volum de servidors virtuals instal·lats, s'ha d'utilitzar l'aplicació de comandes de manera automatitzada amb IaaC (SaltStack i l'eina SyGox), i actualitzar-la afegint funcionalitats necessàries.
- L'administració serà compartida amb l'IMI, que podrà demanar accés root als servidors (amb usuari diferenciat) per poder actuar puntualment sobre els servidors o fer anàlisi de problemes.

Racionalització de la infraestructura

Es fa una revisió periòdica de la infraestructura (com a mínim trimestralment), i es vetlla per tancar aquells servidors i esborrar aquelles configuracions que ja no calguin. Es presenta en el comitè de seguiment tècnic per a la seva discussió i aprovació cas per cas. Inclou tasques específiques com:

- Revisar els servidors no usats (per exemple, de webs tancades, entorns de desenvolupament/formació), per demanar als responsables del web el seu tancament.
- Eliminació dels servidors obsolets
- Propostes de consolidació de webs en infraestructura comú en cas de webs amb molt poca càrrega (<20% del servidor) que no justifiqui infraestructura dedicada. Es dona el cas amb campanyes que ja han acabat.

Gestió de la seguretat

- Vetllar per la seguretat dels webs: aplicació guies de bastionat, estar informat de les alertes de seguretat que apliquin als sistemes gestionats, aplicar mesures correctives a nivell de sistema operatiu, manteniment de la seguretat de les plantilles de nous projectes (tant per AMIs com per imatges docker), revisió de la seguretat, definició de mecanismes de vigilància en front a atacs, suport a estudis forenses que pugui realitzar l'IMI o en qui delegui.
- Facilitar al departament de seguretat de l'IMI, o als encarregats en qui aquest delegui, l'execució de proves de pentesting i/o estudis forenses.

Configuració de frontals

- Configuració de frontals NGINX i/o Apache2 relatives a regles de seguretat, redireccions entre ports HTTP/HTTPS, configuració de virtual hosts, redireccions de



webs obsoletes cap a les corresponents webs noves, configuracions de memòria cau, instal·lació i custòdia dels certificats digitals, configuració de pàgines d'error, configuració dels fitxers de robots.txt (per als cercadors) i fitxers d'autorització de Google Search Console.

- Centralització de la gestió de dominis a les IP elàstiques i/o als frontals, per evitar que el domini apunti directament als servidors d'aplicació, permetent la implementació de seguretat perimetral, i permetent la portabilitat d'aplicacions a diferents servidors sense haver de modificar els DNS.
- Separació d'entorns de desenvolupament dels entorns productius mitjançant la configuració de dominis separats (amb el prefix "dev-", com per exemple: "dev-ajuntament.barcelona.cat"). Els entorns de desenvolupament hauran d'estar sempre protegits per contrasenya, per evitar que un visitant arribi accidentalment.
 - Caldrà habilitar mesures (per exemple xarxes privades virtuals [VPN]), d'acord amb les directrius i requeriments que marqui l'IMI, per tal que aquest entorns siguin accessibles només pels programadors i no siguin accessibles des d'internet.
- Separació de la funcionalitat d'entrada de continguts i configuració dels webs de la part pública visible dels webs, mitjançant la configuració de dominis separats (amb el prefix "continguts-", com per exemple: "continguts-ajuntament.barcelona.cat"). Les pàgines de identificació d'usuari i la funcionalitat d'administració haurà d'estar capada al domini públic, per evitar que s'hi pugui accedir accidentalment o es puguin rebre atacs maliciosos si el desenvolupador no el desactiva.
 - Caldrà habilitar mesures (per exemple xarxes privades virtuals [VPN]), d'acord amb les directrius i requeriments que marqui l'IMI, per tal que aquest entorns siguin accessibles només pels contribuïdors de contingut, i no siguin accessibles des d'internet.
 - Caldrà habilitar mesures per evitar atacs de força bruta en el descobriment de contrasenyes, detectant i bloquejant intents d'intrusió sistemàtics.
 - Caldrà que les aplicacions que comparteixen mateix domini per mantenir (com es per defecte en Drupal/wordpress), es donin les indicacions adequades als programadors per aconseguir aquesta separació d'entrada alternativa als redactors.
- Automatització de les configuracions dels frontals, per guanyar en agilitat, en documentació, i per possibilitat l'autoprovisió en els casos més comuns.
- Configuració i custòdia dels certificats digitals.

Verificació de Còpies de seguretat

- Cal vetllar per un bon funcionament del sistema de còpies de seguretat, i dur a terme revisions periòdiques de la configuració i de l'execució per tal d'assegurar que tota la informació s'està guardant correctament, que la informació és completa, íntegra, i que la informació és suficient per al restabliment del web.



- La política de còpies actual es basa en retenir una còpia de seguretat diària de la última setmana, una còpia de seguretat setmanal de l'últim mes, i una còpia de seguretat mensual de l'últim any.
- En els projectes d'arquitectura dedicada, tots les còpies de seguretat són complets (no incrementals) i inclouen la configuració del webserver, el docroot, i la base de dades. Exclouen explícitament la còpia de certificats digitals que hi pugui haver.
- En els projectes consolidats, les còpies de seguretat són incrementals. Les configuracions es guarden al repositori de codi GIT, donat que la creació de la infraestructura i la configuració es fa per codi (salt stack).
- Cal revisar, amb periodicitat setmanal:
 - Que els projectes productius tenen les còpies de seguretat activades
 - Que tots els directoris d'informació i configuració estan inclosos als còpies de seguretat
 - Que els certificats digitals custodiats estan exclosos de les còpies de seguretat (per directius de seguretat)
 - Que no hi ha incidències en les còpies de seguretat periòdiques i s'han realitzat tots correctament (per exemple, per problemes de connectivitat, de poc espai de disc, falla del cron, etc.)
- Cal comprovar, amb periodicitat mensual:
 - Realitzar una prova de recuperació d'un web elegit a l'atzar en un nou servidor creat temporalment, i comprovar el bon funcionament. S'anotaran en un informe breu les incidències trobades (si és el cas), i el temps emprat en la recuperació. Un de cada tres vegades com a mínim es triarà un web de talla estratègica. La prova consistirà com a mínim en validar un total de 10 pàgines incloent la home, tant visualment com tècnicament (amb la consola del desenvolupador del navegador) comprovar que no hi ha elements que faltin o crides que fallin, i realitzar una cerca en el web (si hi ha aquesta funcionalitat).
 - Les còpies de seguretat haurien d'estar preparades davant d'atacs de "ransomware" habilitant per exemple el versionat dels backups, o usant medis extraïbles o allotjaments alternatius totalment desconectats de la infraestructura.

Custodia de certificats digitals

- En determinats webs o dominis, s'emet un certificat digital de domini o d'organització. Aquests certificats els custodia l'administrador del sistema, i realitza auditories periòdiques per comprovar que es segueixin complint els requisits de seguretat acordats.
- Les tasques a dur a terme respecte la custòdia, són:
 - En el cas de nou certificat, gestió de la petició de certificats al departament de seguretat de l'IMI: complimentar el document de custodiat
 - Definir i implementar la seguretat pertinent del servidor per allotjar els certificats



- Auditar com a mínim mensualment que es compleix la seguretat implementada a tots els certificats custodiats
- Com a norma general, les mesures de seguretat implementades al servidor que allotjarà el certificat, són:
 - El certificat està instal·lat en un sol servidor*
 - El servidor està dedicat per la funcionalitat descrita, i no hi ha cap més servei o web.*
 - Només tindrà accés al directori del certificat l'administrador de sistemes.*
 - Els programadors no tenen accés a l'entorn productiu, que és l'únic que allotjarà el certificat.*
 - Gestió del canvi: Els desplegaments (en el cas del cercador) es realitzen mitjançant scripts automatitzats (implementats amb fabric) que no poden accedir al directori del certificat.*
 - Es treu accés de lectura al fitxer del certificat, per 'others'. Els usuaris per altres processos (ex: nagios) no hi tenen accés.*
 - No es podrà usar aquest servidor com a plantilla de cap altre projecte.*
 - Les còpies de seguretat són de dades, no inclouen el sistema operatiu i per tant no és fa còpia de seguretat del certificat ni s'allotja en cap més banda.*

Modificacions de Sistemes (DNS, registres SPF,)

- Suport a la definició de configuracions DNS per al bon funcionament del servei, en quant a IPs de resolució dels dominis, i configuració de serveis de correu de sortida, de delegació en servidors externs, i d'entrada
- Les modificacions dels DNS els realitza l'IMI o via proveïdor de dominis.

Manteniment de l'inventari de servidors i webs

Inclou les tasques de vetllar per la vigència de l'inventari de servidors, de webs, i de monitors.

Sygox guarda la relació de servidors i de webs que aquest conté, però cal anar modificant l'estat del projecte (desenvolupament, producció), anotar URLs de noves webs incloses (en el cas de compartir el servidor amb varies webs)

Donat els diferents casos i configuracions que es van donant, i la ràpida evolució dels serveis, poden donar-se casos en què les webs quedin amagades, o que segueixin constant un cop tancades, i cal assegurar que tot està ben documentat i que l'inventari és vigent.

Manteniment d'un catàleg de tecnologies disponibles

Inclou les tasques de mantenir un inventari de productes i versions que estan desplegats a tota la plataforma, i d'estandarditzar al màxim la base dels projectes per tal de disposar del mínim nombre de variacions de productes i versions.



Es mantindrà un “catàleg de tecnologies” per als programadors amb les possibilitats disponibles, i totes les excepcions hauran de ser ben justificades, aprovades en el comitè de seguiment, i després incorporades en el catàleg, ja sigui com a nova solució transversal, ja sigui anotat com a excepció puntual.

(Serveis d'Administració de Sistemes): Administració de webs CMS i aplicatius LAMP

Al departament es gestionen prop de 1.050 desplegaments d'Aplicacions Web. Generalment són CMS (Sistema de gestió de continguts) i, d'aquests, el 70% són Drupal i la resta WordPress. El ratio de visites és molt variable, A les webs principals permanents pot ser de 400.000 visites/mensuals. I les Webs d'esdeveniments, tot i ser temporals, poden arribar a milions de visites en pocs dies (Mercè, Grec, Cavalcada dels Reis...). A l'**annex 9** es detalla documentació ampliada que es pot demanar per tenir el detall del llistat dels webs, la tecnologia base de cada una, i una estimació promig de les visites mensuals de cada una.

El gran nombre de pàgines desplegades, la quantitat i l'oscil·lació de tràfic, i la seva fragmentació degut a les diferents tecnologies utilitzades, fa que les tasques d'administració siguin complexes, variades i, en moltes ocasions, es requereixin actuacions urgents i crítiques.

Funcions principals

- Automatitzar l'operativa habitual (per exemple: altes/baixes/petició credencials), per tal que els responsables de l'IMI puguin dur a terme autoprovisionament via l'eina SyGox.
- Assegurar que el rendiment dels webs és bo, aplicant mesures d'optimització (per exemple, aplicació de memòria cau, desactivat opcions debug, suggeriments a programadors).
- Mantenir una guia de bones pràctiques de desplegament
- Donar suport a problemes de funcionament o de rendiment a la plataforma

Casos d'ús més habituals:

Còpia de portals

En el cas de la infraestructura dedicada:

- Realització de snapshots, i/o clonat de webs en nous servidors, per tal de proporcionar entorns de desenvolupament, entorns de diagnòstic, o bé entorns per anàlisi forense.
- Es mantindrà una relació de còpies actives de backup , a fi de comprovar periòdicament si són vigents (com a mínim trimestralment) , i procedir al seu esborrat si ja no estan usades (per evitar costos no necessaris).
- Es vetllarà per no fer duplicats, ni snapshots d'infraestructures que continguin certificats digitals, o en cas de ser necessari, caldrà informar-ho prèviament al



departament de Seguretat de l'IMI, per complir amb les condicions de custòdia del certificat.

Actuacions de Seguretat respecte servidors compromesos

- En cas de resultar un servidor compromès (per atac, virus, o manipulació del contingut), premiarà la directiva de salvaguardar la imatge de l'Ajuntament, comunicar immediatament la incidència al departament de seguretat de l'IMI, i conservar una còpia exacte dels servidors involucrats, per salvaguardar les evidències, i possibilitar l'anàlisi forense i les actuacions legals si es dóna el cas.

De manera coordinada amb el departament de seguretat de l'IMI, i el responsable del web, es seguiran els passos:

- tancar el web o servidor, donant una pàgina d'avís de «no disponible temporalment»
- comunicar a IMI seguretat la incidència, aportant la màxima informació rellevant: web afectada, servidors afectats, si es compromet o no el ciutadà, com s'ha arribat a detectar, data estimada de la incidència
- guardar còpia exacta dels servidors afectats intacta (snapshot).
- contactar amb els responsables del web per procedir a la neteja o restauració del servei.
- Suport en el diagnòstic de l'afectació
- en cas de ser demanat pel responsable del web, restauració de còpies de seguretat en un servidor nou (per tal d'eliminar tota possibilitat d'infecció del sistema) i renovació de credencials de l'aplicació
- gestió de la incidència de seguretat amb IMI, donant suport al forense i a l'informe final, fins al seu tancament

Consolidació de webs (de dedicat a consolidat)

Aquesta tasca consisteix en incorporar webs des de servidors dedicats al servidor consolidat, sempre que sigui adequat i possible, a fi de tenir una infraestructura menor i més estandarditzada.

Recuperació de còpia de seguretat

- En cas de sol·licitar-ho pel responsable d'un web, o detectar per un error que el web ha quedat corrupte, es pot dur a terme la recuperació d'una còpia de seguretat.
- Es fa amb l'eina SyGox, i el procediment seria:
 - Assegurar que es disposa d'una còpia de seguretat del servidor actual a esborrar (malgrat estigui compromès o corrupte), tant del frontal com de la base de dades.
 - Cal marcar aquesta còpia de seguretat com a permanent (que no s'esborri amb la rotació). Es guarda per possibles referències fins a la total recuperació i tancament de la incidència per totes les bandes.



- En cas de recuperació per intrusió/virus, cal guardar un snapshot exacte del servidor i la seva base de dades (per dur a terme l'anàlisi forense), tant del frontal com de la base de dades.
- Mitjançant l'eina SyGox, es demana al sistema una restauració d'una còpia de seguretat amb data concreta (a consensuar amb el responsable del web), que el sistema realitza de manera automàtica. Pot ser només del frontal, o també de la base de dades, segons el cas i la incidència que el motiva. També es pot dur a terme sobre el mateix servidor o sobre un de nou.
- Cal gestionar la distribució de noves credencials amb els programadors si es dona el cas de canvi de servidor.

Suport a grans esdeveniments i a situacions crítiques de la ciutat

Implica dedicar un esforç especial en dedicació i increment d'infraestructura arrel de campanyes rellevants que es puguin produir per web, i que eventualment provoquen altes concentracions de visites, o bé en ocasió d'actuacions tècniques sensibles.

Alguns d'exemples de moments que han requerit dedicació especial:

- Migració de domini "web ajuntament" i barres corporatives
 - Migració domini "lameva" a "www"
 - Esdeveniments: La Nit del Museu, Festival DAU, LlumBCN, Festival Grec
 - Esdeveniment: Festes de La Mercè
 - Eleccions
 - Esdeveniment: Mapa recorregut cavalcada dels reis (nadal)
- Altres: circumstàncies especials no previsible (ex: nevades, alertes contaminació, alertes de seguretat ciutadana)

Gestió de configuració de sondes de monitorització web

Inclou les tasques de configurar les sondes pertinents per tal de mantenir tota la plataforma correctament controlada, i de rebre avisos automatitzats en cas d'incidència, i de poder obtenir informes de disponibilitat.

Es disposa de varis sistemes de monitorització per tal d'assegurar un correcte funcionament de la infraestructura i dels webs que s'hi allotgen. Els dos principals són el nagios (dins la pròpia infraestructura) i l'uptimerobot (servei extern).

El sistema nagios està orientat a monitorització de baix nivell (CPU, RAM, disc), detecció de conflictes, i gestió automàtica en cas de mal funcionament (reiniciat de webserver en cas de bloqueig).

Es disposa d'un servei de monitorització extern, l'uptimerobot, que realitza la validació dels webs des del punt de vista de visitant web.



Cal vetllar per tal que tots els projectes tinguin ben configurades aquestes sondes, i que el seu resultat sigui significatiu per fer seguiment de disponibilitat.

Cal verificar:

- Que cada web tingui les sondes correctament configurades, tant de visitant (uptimerobot) com de servidor (nagios)
- Que es detecti no només indisponibilitat de la pàgina, sinó també altres casuístiques errònies malgrat retornin codi HTTP 200. Això es fa mitjançant la validació d'una paraula clau fixa de la pàgina.
- Que es desactiven les sondes obsoletes (de les webs que s'han despublicat o migrat a nous servidors).
- Que les sondes de sistema (nagios) estiguin actives per tots els entorns productius, i que estiguin habilitats els serveis automàtics d'actuació en cas de bloqueig.

Gestió de la comunicació d'indisponibilitats/baix rendiment dels webs (grafana)

Inclou les tasques de revisar setmanalment la disponibilitat i el temps de resposta dels webs, en base al report setmanal proporcionat pel servei nagios i grafana. S'analitzaran les incidències i es valorarà per tots aquells que es consideri problemàtics, d'escalar-ho als responsables del web per tal que es revisi la programació del web.

Es considera que el temps de generar i servir completament una pàgina dinàmica, especialment per les homes dels webs, ha de ser de un màxim de **3 segons**. Es vol identificar i escalar els casos en que aquest requeriment no es compleixi.

En d'altres casos, per incidències imputables a la infraestructura, es procedirà a la seva reparació.

Per tots els casos oberts, es mantindrà un registre i es revisaran setmanalment fins a la seva resolució total i que els reports de disponibilitat siguin favorables.

Disseny de bones pràctiques per al rendiment i mantenibilitat

Inclou les tasques de mantenir una documentació que permeti al programador web desplegar fàcilment el seu web a la infraestructura, i fer una configuració òptima que maximitzi el rendiment i la mantenibilitat futura.

3.5.2. Suport

3.5.2.1 Help Desk

El servei de Help Desk consisteix en oferir a l'usuari d'un mètode de comunicació eficaç per comunicar incidències, problemes i dubtes.



Els Serveis Transversals de Manteniment (STM) seran responsables de la gestió del servei de Help Desk del SAU específic. Aquest servei inclou les activitats de:

- Recepció de les incidències o consultes (relatives al servei de la present licitació) rebudes del SAU IMI/Ajuntament.
- Resolució de les incidències o consultes i reassignació de les que no li corresponguin.
- Documentació de les incidències en els sistemes i eines proporcionades per l'IMI.
- Seguiment i informació de les incidències derivades a altres grups fins el seu tancament.
- Gestió del tancament de les incidències en el sistema de gestió d'incidències i comunicació a l'usuari de la seva resolució.

Aquestes activitats es realitzaran en horari laboral i sota les condicions establertes a l'apartat "4: Condicions generals de la prestació del servei" del present document.

En el present contracte l'adjudicatari es relacionarà amb aquest servei d'atenció a l'usuari de l'IMI:

- SAU IMI/Ajuntament de Barcelona: Serveis de gestió d'atenció a l'Usuari de l'Ajuntament de Barcelona, el qual dona servei als usuaris interns de l'Ajuntament i realitza els serveis de gestió i operatius: gestió dels serveis operatius, centre de serveis, helpdesk de primer nivell, helpdesk de segon nivell, activitats de suport in-situ i manteniment d'infraestructures. **La realització d'aquest servei de SAU IMI a tot l'Ajuntament de Barcelona està fora de l'abast del present contracte.** Únicament s'hauran de gestionar, tractar i resoldre les incidències relatives al servei relacionat amb el present contracte que es derivin a l'adjudicatari i donar resposta al tancament de les mateixes en la plataforma del SAU IMI.

3.5.2.2 Suport funcional

Els Suport Funcional inclou les següents tipologies de tasques:

- Suport als usuaris en el funcionament de les aplicacions, resolent els dubtes de manera puntual que puguin aparèixer respecte al funcionament de les mateixes.
- Assistència i acompanyament en les reunions i preparació d'informació de suport, sota demanda de l'IMI. En el cas que una assistència requereixi un esforç superior a 3 jornades d'horari base (veure apartat 4.2.1 del present plec) de suport funcional, es gestionarà via manteniment recurrent.
- Realització d'ajustos adaptatius, parametritzacions i petites millores funcionals, de poc esforç d'implantació i alt benefici per l'usuari. S'estima un esforç màxim de **10 hores de treball** per cada suport d'aquesta tipologia. Si s'estima més esforç es gestionarà com manteniment recurrent.
- Tasques d'**estimacions**: L'adjudicatari realitza un primer anàlisi ràpid de la necessitat del manteniment recurrent i presenta una **estimació** a l'IMI que detalla el nivell (baix,



mig, alt) de complexitat de la solució (pot incloure diferents alternatives). **I es reporta com Servei Transversal de Manteniment.**

- Les tasques incloses en la devolució del servei.

És obligació de l'adjudicatari donar resposta a les peticions de tasques de suport funcional en menys de **5 jornades d'horari base** (per l'horari veure apartat **4.2.1** del present plec) (veure ANS Pet Treso, apartat **8.1.4** del present document).

L'adjudicatari haurà d'identificar i proposar en el Comitè de Direcció proactivament accions formatives i de comunicació que puguin millorar el suport funcional de forma preventiva i que permetin reduir el nombre de casos de suport funcional rebuts.

El licitador haurà de presentar una proposta de diagrama de flux i dels procediments associats al Suport Funcional. Es valorarà la claredat del diagrama plantejat i que els procediments siguin el més complets possibles i aplicables en un entorn com el de l'IMI.

3.5.2.3 Suport tècnic

El subservei de suport tècnic inclourà també:

- Col·laboració obligatòria en auditories i contra valoracions que s'encarreguin a tercers.
- Tasques de valoració de manteniments recurrents que no s'acaben implementant. En cas que el manteniment recurrent al final no es realitzi, el tiquet amb les seves imputacions d'hores es canviarà com a servei de contracte de Serveis Transversals de Manteniment (STM), tasca de suport tècnic.
- Realització d'ajustos tècnics, parametritzacions i petites millores tècniques, de poc esforç d'implantació i alt benefici per l'usuari. S'estima un esforç màxim d'1 jornada d'horari base (veure apartat **4.2.1** del present plec) per cada suport d'aquesta tipologia. Si s'estima més esforç es gestionarà com manteniment recurrent.
- Assistència i acompanyament en les reunions tècniques de qualsevol direcció/departament de l'IMI/Ajuntament i preparació d'informació de suport, sota demanda de l'IMI. En el cas que una assistència requereixi un esforç superior a 3 jornades d'horari base (veure apartat **4.2.1** del present plec) de suport tècnic, es gestionarà via manteniment recurrent.
- Tasques d'estimacions: L'adjudicatari realitza un primer anàlisi ràpid (que no superi les 8 hores de feina) de la necessitat del manteniment recurrent i presenta una estimació a l'IMI que detalla el nivell (baix, mig, alt) de complexitat de la solució (pot incloure diferents alternatives). I es reporta com Servei Transversal de Manteniment.
- Les tasques incloses en la devolució del servei.
- Tasques d'extracció d'informació sol·licitades per l'usuari o tasques de poc esforç d'execució i alt benefici per l'usuari. S'estima un esforç màxim d'1 jornada d'horari base (veure apartat **4.2.1** del present plec) per cada suport tècnic d'aquesta tipologia. Si s'estima més esforç es gestionarà com manteniment recurrent.



3.5.2.4 Coordinació de la documentació

El Servei de Documentació inclou:

- La generació i actualització de la documentació relacionada amb els manteniments que es realitzin en el transcurs del contracte i que forma part del seu lliurament (inclosa en l'elaboració de cada manteniment recurrent).
- La documentació de la resolució d'incidències, entre elles la identificació proactiva d'errors coneguts (inclosa en les tasques de cada manteniment correctiu).
- La documentació de les aplicacions que són objecte del contracte si la documentació fos inexistent o obsoleta, sempre d'acord en contingut i abast de l'actualització amb el responsable del servei de l'IMI (inclosa en les tasques de manteniment recurrent – deute tècnic o funcional).

Serà responsabilitat de l'adjudicatari l'actualització de la documentació de totes les aplicacions (documentació APP) incloses en el plec durant el transcurs del contracte.

Serà responsabilitat de l'adjudicatari presentar al comitè de direcció el detall de la documentació actualitzada/generada semestralment, en funció de les tasques realitzades. Aquesta informació haurà de ser preparada per l'adjudicatari i validada amb el responsable del contracte amb anterioritat al comitè de direcció.

La documentació generada es farà en format editable i PDF, segons indicacions proporcionades per l'IMI. Aquesta documentació es mantindrà actualitzada a les eines que l'IMI proveeixi als proveïdors. En general, a nivell orientatiu és necessari per a cada aplicació del present plec, segons criteri del responsable del servei de cada sistema, la següent documentació:

- Documentació funcional
- Document d'arquitectura, pla d'infraestructures i entorns
- Pla de proves
- Disseny tècnic
- Guia de parametrització
- Actualització de Manuals d'Usuari
- Catàleg d'interfícies
- Inventari de processos batch
- Inventari de plantilles
- Rols i autoritzacions
- Manual d'exploració

L'IMI comunicarà a l'adjudicatari l'estructura mínima que hauran de tenir els documents anteriors.

En el cas que ja existeixi documentació, aquesta documentació haurà de ser mantinguda i evolucionada en funció dels treballs realitzats.



En l'àmbit d'aquest contracte l'IMI podrà decidir en cada cas (evolutiu, petició de manteniment o incidència) si la documentació del contracte es realitza utilitzant plantilles i documents, o si bé s'utilitzen eines de gestió específiques per a cadascun d'ells.

L'IMI de forma explícita subministrarà eines per al registre de gestió de requeriments, proves i defectes tal i com s'indica en l'apartat 6 Eines del Servei, que podran ser d'obligat ús cas que l'IMI així ho decideixi.

El proveïdor atindrà els processos de Gestió Documental de l'IMI que siguin d'aplicació en el present plec, en especial aquells relacionats amb la incorporació automàtica de la documentació a la gestió del coneixement.

Tota la documentació creada o actualitzada en el desenvolupament del contracte serà propietat de l'IMI.

En cas que la documentació generada manifesti mancances de qualitat, la revisió i correcció de les mateixes correrà a càrrec de l'adjudicatari, a banda de l'aplicació del corresponent ANS.

3.5.3. Gestió del canvi

3.5.3.1 Comunicació

Els Serveis Transversals de Manteniment seran responsables, sota les indicacions que proporciona l'IMI, d'aplicar les directrius i demandes d'accions de comunicació, incloent la definició dels col·lectius implicats, canals de comunicació disponibles, facilitadors de les accions de comunicació, resultats i impacte esperat de cadascuna de les accions de comunicació, amb l'objectiu de mantenir informat al col·lectiu d'usuaris afectat dels principals canvis i manteniments que es realitzin.

Serà responsabilitat dels Serveis Transversals de Manteniment facilitar tota la informació rellevant dels serveis del contracte, facilitant la informació i el coneixement del seu estat als interlocutors corresponents de l'Organització Municipal.

Es definiran les actuacions concretes de cada àmbit i els diferents canals mitjançant el treball amb els equips directius dels diferents òrgans afectats segons l'abast organitzatiu.

3.5.3.2 Coordinació de la transició del servei

La transició del servei és la fase d'execució del servei durant la qual es procedeix a traspasar la prestació del servei entre l'adjudicatari sortint i el nou adjudicatari.

Li correspon als Serveis Transversals de Manteniment de l'adjudicatari del present contracte liderar i assegurar que la transició del servei, desplegada dins de les tasques de Manteniment Recurrent – Transició, es realitza assegurant la qualitat i transparència del procés.



La transició es realitzarà de manera particular per cada servei d'aplicació que compongui el contracte. D'aquesta manera, les diferents durades de la transició s'hauran d'ajustar per tal que totes les transicions a realitzar finalitzin a temps per iniciar la prestació del serveis a la data requerida.

La transició (recepció o devolució) de cada servei-aplicació únicament es farà efectiva quan l'adjudicatari sortint i el nou adjudicatari siguin proveïdors diferents. Quan hi hagi continuïtat de proveïdor, aquesta tasca no caldrà executar-la i s'aplicarà la modificació per disminució prevista per aquesta casuística.

S'entén que hi ha continuïtat de proveïdor davant els següents supòsits:

- És el mateix proveïdor el sortint que l'entrant
- El proveïdor entrant forma/va part de la UTE del proveïdor sortint
- El proveïdor sortint forma/va part de la UTE del proveïdor entrant
- El proveïdor sortint és subcontractat pel proveïdor entrant
- El proveïdor entrant i el sortint formen part del mateix grup empresarial

En el cas particular que algun dels proveïdors adjudicataris entrants hagi format part de l'UTE adjudicatària sortint, però fos necessari realitzar la transició d'algun servei-aplicació, aquesta es realitzarà a càrrec de l'adjudicatari i sense cost addicional per l'IMI.

Alhora que l'adjudicatari sortint continua prestant el servei sota les condicions expressades en el present plec, haurà d'assegurar un correcte traspàs de la informació i dels serveis al nou adjudicatari.

L'adjudicatari haurà d'elaborar el Pla de Recepció/Devolució del Servei sobre el conjunt dels treballs previstos en el plec per si es dona la hipòtesi de canvi d'operador a l'inici d'aquest servei, finalització d'aquest contracte o finalització de les possibles pròrrogues, si és el cas.

Una vegada adjudicat el contracte resultant d'aquest procés de contractació:

- **En cas de nou proveïdor entrant haurà de presentar el Pla de recepció del servei en la primera setmana del contracte per adaptar el Pla de recepció presentat en fase d'oferta al pla de devolució del proveïdor sortint.**
- **L'adjudicatari haurà de presentar el Pla de devolució del servei, 6 mesos abans de la finalització del contracte.**

El Pla de recepció/devolució haurà de ser aprovat per IMI.

El Pla de recepció haurà de complir, com a mínim, els següents requisits:

- Adequació a les característiques del servei a recepcionar. El Pla de recepció definitiu haurà d'estar personalitzat a les necessitats i requisits del propi servei.
- Detallat a nivell de servei-aplicació.
- Període mínim d'1 setmana i un màxim de 1 mesos segons el servei-aplicació, a determinar amb l'IMI.



- Equip necessari per garantir la recepció del servei.
- Proposta de Model de gestió i coordinació de cada servei-aplicació, detallant els diferents stakeholders (IMI, Ajuntament de Barcelona i altres actors implicats en el servei).
- Planificació i calendari de treball amb reunions, tasques i sessions de formació.
- El traspàs es realitzarà durant l'horari del servei a les oficines que l'IMI determini.
- Planificació de recursos inclosos en la recepció del servei.

El Pla de devolució, haurà de complir, com a mínim, els següents requisits:

- Adequació a les característiques del servei a traspassar. El Pla de devolució definitiu haurà d'estar personalitzat a les necessitats i requisits del propi servei.
- Detallat a nivell de servei-aplicació.
- Període mínim d'1 setmana i un màxim de 1 mesos segons el servei-aplicació, a determinar amb l'IMI.
- Equip necessari per garantir la devolució del servei.
- Documentació actualitzada sobre les aplicacions dins de l'abast: funcional, tècnica, operativa, etc.
- Configuració i detall dels entorns de treball.
- Estat de les incidències, problemes o tasques obertes en el moment de la devolució.
- Model de gestió i coordinació de cada servei-aplicació, detallant els diferents stakeholders (IMI, Ajuntament de Barcelona i altres actors implicats en el servei).
- Històric de volumetries de peticions, entrades, sortides, estoc, tasques recurrents.
- Memòries anuals.
- Informes estratègics.
- Bones pràctiques i lliçons apreses.
- Planificació de reunions.
- Planificació i contingut de formacions al nou adjudicatari.
- El traspàs es realitzarà durant l'horari del servei a les oficines que l'IMI determini.
- Planificació de recursos inclosos en la devolució del servei.

Durant l'execució del Pla de devolució l'adjudicatari sortint ha d'assegurar la continuïtat del servei amb el compliment dels ANS establerts per a cadascun dels serveis i totes les responsabilitats per a la seva correcta execució, tal i com s'especifica en el present plec. L'adjudicatari sortint és ple responsable del servei.

En el moment d'acceptació de la transició del servei es conformarà l'acta de recepció a partir de quan el proveïdor entrant passaria a ser responsable del servei amb aplicació dels ANS corresponents. En cas de continuïtat de proveïdor també caldrà conformar formalment aquest acta per consolidar canvis d'equips si fos el cas.

3.5.4. Gestió del contracte



3.5.4.1 Reporting

Els Serveis Transversals de Manteniment seran els encarregats de la preparació i presentació de la documentació requerida en els diferents comitès estipulats en l'apartat **5.2** Model de govern del present plec de prescripcions tècniques. La informació subministrada a l'IMI haurà de ser en format editable i haurà d'incloure tota la informació de referència que ha permès la seva elaboració.

A continuació, es detalla el contingut mínim dels diferents informes:

3.5.4.1.1 Informe Comitè de Seguiment Operatiu

Informe descriptiu de l'execució del servei durant el període. L'informe de seguiment haurà de presentar-se en el Comitè de Seguiment tal i com s'estipula en l'apartat **5.2** (Model de Govern).

Aquest document haurà d'incorporar com a mínim els següents punts

- Seguiment operatiu
 - 1.– Revisió acords i temes pendents comitè anterior
 - 2.– Anàlisi situació:
 - Estat incidental
 - Revisió problemes i estat problemes en curs
 - Recurrents en curs i planificats
 - Tiquets en garantia
 - Estat *pending others/customer*
 - Radar del servei (temes a comentar)
 - Consum per servei respecte LB
 - Facturació/ANS
 - 3.– Anàlisi demanda:
 - Planificació de tasques
 - Nova demanda i estimacions
 - 4.– Altres aspectes rellevants

3.5.4.1.2 Informe Comitè Tècnic

Informe descriptiu de temes tècnics i de coordinació tècnica del servei durant el període. L'informe de seguiment haurà de presentar-se en el Comitè Tècnic tal i com s'estipula en l'apartat **5.2** Model de Govern .

Aquest document haurà d'incorporar com a mínim els següents punts

- Seguiment tècnic
 - 1.– Revisió acords i temes pendents comitè anterior
 - 2.– Anàlisi situació:
 - Relació de temes tècnics:



- Descripció, Estat, Planificació, Realització, Responsable, Impactes i dependències
- Riscos identificats i proposta de solucions

3.5.4.1.3 Informe Comitè de Direcció

Informe descriptiu de l'execució del servei durant el període. L'informe de seguiment haurà de presentar-se en el Comitè de Direcció tal i com s'estipula en l'apartat 5.2 Model de Govern.

Aquest document haurà d'incorporar com a mínim els següents punts:

- Seguiment executiu:
 - Revisió acords i temes pendents comitè anterior
 - Visió global AM
 - Quadre de comandament global del servei (veure apartat 3.5.1.1)
 - Proposta de facturació
 - Acords de Nivell de Servei i tiquets en garantia
- Seguiment operatiu:
 - Visió global i detall per servei de contracte
 - Projectes
 - Anàlisi compromès-executat
 - Situació de contractes
 - Equip de treball de l'AM i imputació d'hores reals de cada treballador/a del contracte
 - Revisió *Pending others/customer*
 - Pla de monitorització del servei (veure apartat 3.5.1.5)
 - Previsió tasques per els propers mesos
 - Altres aspectes rellevants

En document adjunt "Plantilla_Comitè_Direcció_v6_20240201.pptx" es detalla el model d'informe de seguiment pel Comitè de Direcció. L'IMI podrà modificar l'estructura de l'informe i el seu contingut durant l'execució del servei.

3.5.4.1.4 Memòria anual

Una vegada l'any, l'adjudicatari haurà de presentar una memòria en el qual s'indiqui el desenvolupament dels diferents serveis de contracte executats. Aquesta memòria s'entregarà a principi d'any amb el tancament natural anual anterior i a la finalització del contracte s'haurà d'estructurar amb visió global i organitzativa (gerència, direcció/àrea) i haurà d'incloure, com a mínim amb els següents punts:

- Visió global
- Comparativa amb memòria anterior per servei de contracte
- Servei del Contracte: Volumetries i esforços dedicats
- Correctius, Recurrents, Serveis Transversals de Manteniment vs. hores executades



- Correctius, Recurrents, Serveis Transversals de Manteniment vs. nº tiquets
- Acumulació de tiquets creats vs. tancats.
- Acumulació de tiquets reoberts vs. total
- Serveis Transversals de Manteniment al detall
- Tiquets en garantia
- Servei d'Aplicació : Resum dels indicadors d'activitats/ús més rellevants de l'àrea
- Serveis /App vs. Compromès, Executat i Línia Base
- Anàlisi de la dedicació real (executat) en Serveis /App segons tipologia
- Anàlisi del nombre de tiquets creats en Serveis /App segons tipologia
- Evolució de la dedicació de les App més rellevants
- Resum dels riscos i mesures de mitigació
- Resum d'accions de comunicació
- Resum de l'estat de seguretat: riscos, millores aplicades, actualitzacions pendents, propostes de millora
- Formació realitzada
- Millores realitzades
- Millores operatives /administratives
- Millores en Serveis d'Aplicacions
- Fites d'interès
- Valoracions globals

L'IMI facilitarà a l'adjudicatari un document amb les instruccions per realitzar la memòria i les indicacions de com complimentar cada apartat. Aquest document podrà evolucionar durant la vigència del contracte i ser adaptat en el seu contingut a criteri del responsable del contracte.

3.5.4.1.5 Informe de tendències tecnològiques

L'informe de tendències tecnològiques té l'objectiu d'oferir una visió actual i a futur de la tecnologia sobre la qual es desenvolupen les diferents aplicacions. Aquest informe s'entregarà a principis d'any amb el tancament natural anual anterior i a la finalització del contracte i haurà d'incorporar com a mínim els següents apartats:

- Desenvolupament de la tecnologia fins al moment de la redacció de l'informe
- Tendències de futur previstes per a la tecnologia analitzada
- Descripció de les possibles aplicacions de les tendències a futur identificades a les aplicacions
- Fonts d'informació utilitzades

3.5.4.1.6 Informe estratègic

L'objectiu d'aquest informe és poder analitzar i prendre decisions sobre canvis en la prestació dels serveis, prioritzacions d'àrees i sistemes. En aquest informe cal que l'adjudicatari proposi actuacions dins de les classificades com a serveis preventius i perfectius, indicant quin objectiu es persegueix. Aquesta informació s'utilitzarà per acordar i prioritzar actuacions futures.



L'Informe Estratègic és un informe anual que utilitzarà la informació de la Memòria Anual com a informació d'anàlisi de partida, l'informe de tendències tecnològiques com a visió de futur i presentarà les recomanacions concretes a aplicar. Haurà d'incorporar com a mínim els següents punts:

- Resum del desenvolupament dels diferents serveis
- Anàlisi de tendència, incloent volumetries i esforços
- Propostes per reduir el volum d'incidències
- Propostes de millora
- Propostes de formació, gestió del canvi o documentals
- Propostes de reorganització d'equips o volumetries de serveis
- Propostes per reduir riscos identificats

L'IMI podrà demanar a l'adjudicatari la creació d'informes i documentació addicional o amb una altra periodicitat, sense que això suposi una despesa addicional.

3.5.4.2 Indicadors del Servei – Quadre de seguiment del servei

De cara al tancament mensual del servei i la preparació de la proposta de facturació, a nivell operatiu caldrà treballar i actualitzar les dades mensuals i acumulades relatives a l'estat del servei tant a nivell quantitatiu com qualitatiu. L'actualització d'aquestes dades seran preferiblement i majoritàriament automàtiques, i serà responsabilitat de l'adjudicatari verificar i analitzar les dades obtingudes i realitzar la seva distribució al responsable del contracte, responsable sectorials i responsable del servei:

- Proposta de facturació mensual
- Seguiment econòmic mensual i acumulat per Correctiu, Recurrent, STM i total d'executat vs. línia base i desviacions.
- Seguiment d'hores mensual i acumulat per Correctiu, Recurrent, STM i total d'executat vs. línia base i desviacions.
- Distribució d'hores planificada i real
- Evolucions d'estocs mensual i acumulada: Entrades, Sortides i Estoc per Correctiu, Recurrent i STM
- Temps de resposta i tancament dels tiquets i desviacions de Manteniment Correctiu i Recurrent
- Anàlisi de les tipologies i mides dels tiquets, diferenciant Correctiu, Recurrent i STM
- Promig d'hores dedicades als tiquets per servei, diferenciant Correctiu, Recurrent i STM
- Diferència estimacions Manteniment Recurrent respecte a execucions
- Tasques de Manteniment Recurrent més rellevants en curs o tancades en el mes
- Tasques de Manteniment Recurrent cancel·lades
- Garanties i Penalitzacions detallades, tant mensual com acumulades
- Planificació de Manteniment Recurrents en el proper trimestre
- Identificació de tasques de Manteniment Recurrent amb data de lliurament passada (pendent de re planificar)
- Identificació de tasques de Manteniment Recurrent no acceptades amb imputacions (pendent d'acceptar)



- Relació de tiquets en estat *Pending Customer / Pending Others*, justificant cada cas

Les dades indicades anteriorment hauran de poder ser analitzables en dos nivells: Direcció (global del contracte) i Operació (servei-aplicació) en base a la classificació dels diferents serveis del contracte.

L'adjudicatari haurà de preparar, lliurar i analitzar tota aquest informació argumentant desviacions, temes destacats i donant resposta a totes les qüestions que responsables de servei, responsable sectorial i responsable de contracte manifesten al respecte i previ al procés de tancament mensual previ als Comitès de Seguiment i Direcció corresponents. Aquesta revisió s'ha de fer durant la primera setmana laborable del mes.

3.5.4.3 Gestió de riscos

Els Serveis Transversals de Manteniment hauran de vetllar per la identificació, gestió i mitigació dels riscos presentat en l'execució i planificació dels diferents serveis del contracte.

Una gestió de riscos implica una anàlisi constant dels riscos existents al servei, la definició i implantació d'uns indicadors que mesurin i avaluin com s'estan executant els serveis i una proposta de solucions mitigadores.

Inicialment, cal fer una identificació i anàlisi dels possibles riscos, planificant la seva mitigació en cas que esdevinguin. Durant l'execució dels serveis del contracte l'adjudicatari haurà de fer la supervisió i control dels riscos i determinant les accions necessàries per mitigar-los o evitar-los.

L'objectiu és oferir una gestió de riscos contínua des de l'inici del servei de transició, fins a la finalització del contracte de manera que l'adjudicatari sigui proactiu i ajudi a la presa de decisions.

3.5.5. Llicències i productes

Els Serveis Transversals de Manteniment seran els encarregats, en cas que així sigui necessari, de la gestió de les llicències i productes, normalment en modalitat SaaS (Software as a Service), específiques en qüestió, a nom de l'Ajuntament de Barcelona.

Per això, els Serveis Transversals de Manteniment hauran de:

- Recepcionar peticions en referència a llicències/productes, principalment altes i baixes.
- Gestionar les peticions referents a llicències amb les àrees o proveïdors corresponents.
- Seguiment i comunicació de les peticions.
- Gestió de l'inventari de llicències / productes i manteniment del mateix.

Si escau, l'adjudicatari haurà de gestionar en el present subservei el cost de manteniment de les llicències/productes existents així com la compra de les noves llicències determinades en la informació específica, indicat a l'Annex 2 del present document i les noves necessitats



identificades durant l'execució del contracte. L'IMI determinarà el calendari de compra de les llicències i productes i haurà d'autoritzar la compra. L'adjudicatari podrà incloure un marge comercial sobre el cost de les llicències que es concretarà en el comitè de direcció, i que en cap cas superarà el 10%.

L'adjudicatari haurà de proporcionar en el marc del seguiment del contracte, informes que indiquin l'estat de l'inventari de llicències /productes, el volum de peticions i el seu estat, així com la seva previsió i estat de facturació.

3.6. Servei d'aprovisionament d'infraestructura

En aquest servei està inclòs la Provisió (i Suport) de maquinari (IaaS) per allotjar tots els webs i aplicatius, a totes les eines necessàries per dur a terme la seva operació, donant compliment total als mínims requerits en el present plec i com a mínim amb totes les especificacions del servei actual en quant a IaaS de web, còpia de seguretat, panell i API. També inclou el servei de suport al correcte funcionament de la infraestructura base.

Aquest servei inclou:

- Provisió infraestructura per webs CMS (per talles)
- Provisió infraestructura de servidors virtuals dedicats (per talles), per allotjar-hi aplicatius amb arquitectura dedicada, i per les pròpies eines de govern de sistema (monitorització, còpia de seguretat, repositoris, inventari, automatització) i del seu emmagatzematge (per talles)
- Programari com a servei (Infraestructura SaaS): Serveis subcontractats, amb el seu propi suport i administració
- Suport a la infraestructura (Suport a les incidències de maquinari)

Queden excloses d'aquest servei tant l'administració del programari d'aquests servidors (queda inclòs a l'abast del servei transversal de manteniment (STM) del present contracte), com la instal·lació de noves eines o l'evolució del sistema (es fa des del servei de manteniments recurrents del present contracte).

A banda, cal servir la demanda creient de nombre de webs a allotjar que es produeixi durant l'execució del contracte.

Veure a l'annex 2, "Volumetries i dates", l'apartat: "Servei d'aprovisionament d'infraestructura", per consultar el detall d'aquests serveis i de les talles que s'especifiquen per cada un.

- **En cas que el licitador proposi migrar a un nou hosting:**
 - En el nou allotjament, el panell de control i les APIs d'accés han d'existir des d'almenys el mateix dia de la formalització del contracte
 - El cost de la migració i de les incidències que se'n puguin derivar, anirà totalment a càrrec de l'adjudicatari
 - Al finalitzar el contracte, ha de facilitar les eines per traslladar els webs cap a una nova ubicació, si fes falta.



El licitador detallarà en la seva proposta els proveïdors concrets d'infraestructura que es proposa a utilitzar durant el contracte, incloent les seves característiques del servei, el moment en el que es preveu la migració, i com es durà a terme

3.6.1. Infraestructura Webs CMS (PaaS)

Infraestructura clúster per donar servei al principal volum de desplegaments web (prop de 1050). Es tracta de webs informatius, basats en gestors de continguts (CMS) Drupal i Wordpress. Per a la seva facturació, s'han classificat els webs en **talles**, segons els seus requeriments de servei. Inclou en el cost el suport tècnic a infraestructura, que no es podrà facturar a banda dins altres serveis del contracte.

3.6.2. Infraestructura Servidors Virtuals Dedicats (IaaS)

Infraestructura específica de servidors i d'emmagatzematge per un conjunt donat d'aplicacions que per la seva càrrega i/o requeriments específics tenen una arquitectura més complexa i una infraestructura dedicada. Inclou el suport tècnic a infraestructura, que no es podrà facturar a banda.

3.6.3. Programari com a servei (SaaS)

Programari com a servei, que cal subcontractar directament a una empresa determinada per requeriments tècnics. Inclou suport tècnic infraestructura i administració de sistemes, delegat en l'empresa subcontractada.

3.6.4. Suport a la infraestructura

Prestar el suport tècnic del servei Hosting IaaS infraestructura (web, còpies de seguretat, panell i API), donant compliment total a les incidències identificades durant l'execució del servei Hosting IaaS, el qual inclou els mínims requerits en el present plec, i com a mínim amb totes les especificacions del servei actual en quant a IaaS de web, còpies de seguretat, panell i API, detallat en l'**Annex 1** (apartat 13.2: Descripció Infraestructura cloud) del present plec.

A continuació es descriuen els requisits mínims a complir per cobrir el servei de suport tècnic. Concretament, les funcions a cobrir són:

- Suport d'incidències del servei Hosting IaaS: escalar al proveïdor de hosting corresponent les incidències tècniques sobre l'entorn i administració dels serveis de maquinari fins a la seva resolució total.
- Monitorització de la salut del maquinari.
- Manteniment del programari dels hipervisors (si s'escau).



4. CONDICIONS GENERALS DE LA PRESTACIÓ DEL SERVEI

4.1. Localització de la prestació dels serveis

Els serveis objecte del contracte es prestaran des de les instal·lacions del proveïdor, essent obligació de l'adjudicatari l'aportació de les eines necessàries per a la prestació d'aquest servei en forma remota i assumint els costos de tots els mitjans necessaris per aquesta modalitat de prestació.

L'adjudicatari haurà d'utilitzar els comptes de correu electrònic de contacte que l'IMI li facilitarà i haurà de facilitar els següents telèfons mòbils pel contracte:

- Número de telèfon mòbil principal de contacte: aquest número haurà d'estar actiu durant l'horari de prestació del servei (horari base i horaris excepcionals).
- Números de telèfons mòbils professionals pels consultors/es assignats als següents perfils del contracte:
 - Cap de projecte/Responsable del Servei
 - Responsable seguretat
 - Atenció usuaris

En les ocasions que es requereixi, es podrà demanar desplaçament a les oficines de l'IMI per a la prestació de les parts del servei que l'IMI consideri, en forma temporal o continuada. També sota circumstàncies excepcionals pot ser necessari el desplaçament a oficines de l'Ajuntament per la prestació d'algun servei de suport, formacions o per dur a terme reunions amb usuaris i serveis. El cost d'aquests desplaçaments seran a cost de l'adjudicatari, sense cost per l'Ajuntament.

En cas que la prestació del servei es realitzi des de les oficines de l'IMI o de l'Ajuntament el prestatari 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.

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. Es detallaran les condicions d'infraestructura necessària per a la prestació del servei.

L'adjudicatari haurà de garantir la possibilitat de treball en remot i modalitat offline per si es donés el cas de fallada o problemes en les comunicacions o plataformes de l'IMI. La configuració d'aquests entorns locals i les llicències associades, en cas de ser necessari, són responsabilitat de l'adjudicatari. En tot cas s'ha d'assegurar la protecció de dades segons el RGPD.

4.2. Horaris de la prestació dels serveis

4.2.1. Horari base



L'horari base de la prestació dels serveis aplicarà per defecte a tots els serveis-aplicació del contracte:

- **Horari base** del servei **10 x 5** (de dilluns a divendres de 8 h a 18 h) laborables a Barcelona.
- Pels serveis de: Aprovisionament d'infraestructura (inclou la disponibilitat de la infraestructura, Suport a la infraestructura, alta disponibilitat de Web tipus Estratègica): 24x7 (a qualsevol hora tots els dies, incloent festius).

L'adjudicatari pot presentar una **millora de l'horari base del servei**. Cal tenir en compte que tots els ANS es computaran a partir d'aquest horari base o del millorat per l'adjudicatari. Veure apartat de criteris de valoració: "millora en l'horari de suport tècnic".

4.2.2. Horaris excepcionals

Són serveis que es realitzen **fora de l'horari de prestació** de cada servei-aplicació i a petició de l'IMI.

Hi ha de dos tipus:

- Serveis extraordinaris:
 - Excepcionalment, i amb avís previ mínim d'un dia, l'IMI podrà requerir l'execució de determinats serveis per a la realització de qualsevol tasca inclosa en l'abast del contracte.
 - Aquests serveis s'imputaran a l'eina de ticketing com tiquets de manteniment recurrent, aplicant el flux definit de manteniment recurrent i s'imputaran el doble de les hores realitzades.
- Serveis de guàrdia:
 - Són serveis de disponibilitat, on en principi no està prevista cap tasca planificada, però pot ser necessari una actuació tècnica. En el cas de ser necessària una actuació tècnica, aquesta es tractarà com un servei extraordinari (detallat a l'apartat anterior).
 - L'IMI comunicarà els serveis de guàrdia a l'adjudicatari amb avís previ mínim de tres dies.
 - Per cada guàrdia l'IMI comunicarà a l'adjudicatari els dies, l'horari i els perfils necessaris per realitzar la guàrdia.
 - Els serveis de guàrdia s'imputaran a l'eina de ticketing com tiquets de manteniment recurrent, aplicant el flux definit de manteniment recurrent i s'imputaran al 25% de les hores de durada de la guàrdia.
 - El personal assignat a la guàrdia ha d'estar a una distància màxima d'una hora al centre de treball determinat a la petició de la guàrdia (ja sigui un centre de l'Ajuntament o un centre de treball remot).

4.3. Idioma



De forma obligatòria, l'adjudicatari desenvoluparà els sistemes i interfícies d'usuari externes en català. L'ús del català aplica també per a la documentació de gestió i per a la documentació tècnica requerida i lliurada durant l'execució del contracte, així com en qualsevol altre comunicació requerida.

4.4. Període de garantia

Les accions de manteniment correctiu que provinguin d'una acció prèvia realitzada pel mateix adjudicatari(*) en el desenvolupament de qualsevol dels serveis definits en el present plec de prescripcions tècniques, es tractaran com a activitats subjectes a garantia, de manera que, tot i haver-se de registrar en els sistemes tal i com s'indica en l'apartat "6. Eines del servei", no es podran compatibilitzar com a esforç subjecte de facturació.

(*) S'entén mateix adjudicatari quan hi ha continuïtat de proveïdor, és a dir, quan es compleix algun dels següents supòsits:

- És el mateix proveïdor el sortint que l'entrant
- El proveïdor entrant forma/va part de la UTE del proveïdor sortint
- El proveïdor sortint forma/va part de la UTE del proveïdor entrant
- El proveïdor sortint és subcontractat pel proveïdor entrant
- El proveïdor entrant i el sortint formen part del mateix grup empresarial

Durant el període de garantia l'adjudicatari es compromet a resoldre totes les incidències o defectes detectats en els desenvolupaments lliurats que li siguin imputables a ell per acció o per omissió, sense cap tipus de cost per a l'IMI.

El període de garantia s'haurà d'executar en els termes estipulats en el present punt, tot i que l'adjudicatari no continuï amb la prestació del servei.

El concepte de garantia s'estén en aquest servei a tot aquell producte generat per l'adjudicatari sigui desenvolupament de codi (sigui manteniment correctiu, manteniment recurrent o evolutius identificats o recurrents) o documents, informes, detall d'estimacions o d'altres, que hauran de se corregits per l'adjudicatari si és degut a manca de qualitat o incompletesa atribuïble al proveïdor, sense cost repercutible a l'IMI.

Les tasques relacionades amb els serveis de manteniment correctiu, recurrent i evolutius identificats, i els seus productes associats, tindran una garantia de **6 mesos**, des de la seva posada a producció a disposició dels usuaris.

Les actuacions subjectes a garantia hauran de ser incorporades com a informació de l'estat dels serveis en els comitès de seguiment indicant el seu període de finalització per servei i estaran subjectes als ANS (veure apartat 8).

En el cas de la realització de tasques de manteniment que tinguin com a origen un desenvolupament realitzat per un altre proveïdor, el període de garantia no aplica.

Aquesta gestió es portarà individualment per a cada servei de manteniment realitzat.



4.5. Arquitectures i infraestructura

4.5.1. Entorn cloud públic AWS

EL cloud públic a AWS és l'entorn gestionat actual per l'adjudicatari d'aquest contracte.

Les plataformes tecnològiques utilitzades per al desenvolupament del contracte en l'entorn actual AWS són les següents:

A nivell de sistemes:

- AWS (EC2, SecurityGroups, VPC, S3, RDS, EKS, ElasticCache, CloudFront, ALB, CloudWatch, ApiGateway)
- Linux (Ubuntu)
- SaltStack
- Terraform
- Docker, Kubernetes

A nivell de base de dades:

- Redis (tant per apps Python internes com per cache a PHPs)
- MySQL (per suport apps PHP)
- PostgreSQL (tant per suport a python Django com per aplicacions internes com Sygox)

A nivell de monitorització, logatge i backup:

- CheckMK
- Telegraf / Grafana / InfluxDB
- Syslog-ng
- Bareos per el backup

A nivell de desenvolupament d'eines de govern:

- Python
- Django
- Flask (Sygox i altres eines no son django sinó flask)
- React (per Sygox)

A nivell de suport a desenvolupament web:

- PHP (per suport apps PHP)
- Drupal
- Wordpress

A nivell d'integració contínua:

- gitlab ci
- SATIS

A destacar el nivell de suport a desenvolupament web en PHP (per Drupal i Wordpress) i eines de govern en Python/Django. A continuació es detallen.



PHP

El llenguatge de programació PHP és dels més utilitzats dintre del ecosistema de cloud públic de l'Ajuntament.

Dintre d'aquest entorn ens trobem diferents frameworks:

- Vanilla PHP
- Drupal
- WordPress
- Laravel

El PHP en la majoria dels casos s'utilitza dintre dels CMS Drupal i WordPress que ocupen un rol fonamental dintre de les que son les aplicacions web de cara al ciutadà, més orientades a la comunicació. Entre els dos CMS, el més utilitzat és el Drupal, actualment tenim uns 700 webs productius aproximadament.

Els webs més recent Drupal es poden desplegar amb integració continua seguint una guia de desenvolupament i pujant el codi dintre del gitlab de l'Ajuntament que es fa càrrec del desplegament.

Tots els CMS i aplicacions PHP tenen la mateixa infraestructura basada en un server web APACHE2, base de dades Mysql, sistema de cache amb Redis i CDN Cloudfront.

Python/Django

L'Ajuntament de Barcelona ha apostat per Python ja que suporta diversos paradigmes de programació, incloent-hi programació orientada a objectes, imperativa i procedimental. Presenta un sistema dinàmic i una gestió de la memòria automàtica i té una gran i exhaustiva biblioteca estàndard, per cobrir el màxim de funcionalitats requerides en l'àmbit públic.

En l'Annex 7 Python, es detalla les recomanacions, normes, versions i d'altres, com a guia per a una correcte implementació de les solucions.

Java J2EE

Per les eines corporatives, no aplica al present contracte.

4.5.2. Entorn Cloud Privat de l'IMI

Aquest és l'entorn gestionat per l'IMI. Pot donar-se el cas de que calgui conèixer aquesta arquitectura per integrar un servei del cloud privat amb un servei de l'IMI.

Per treballar en aquest entorn s'hauran de seguir els estàndards definits per l'IMI.

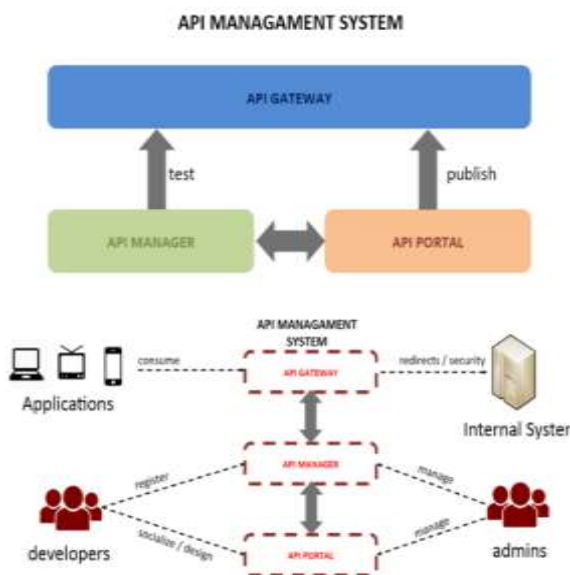


4.5.3. Estàndards d'integració: API Manager(API Connect)

Tot el negoci del sistema d'informació o aplicació ha de ser publicat i consumit mitjançant API(s).

Totes les API(s) per motius de Seguretat i gestió s'han de publicar en l'API Manager estàndard de l'IMI i s'han de consumir única i exclusivament per aquest API Manager.

L'IMI disposa d'un únic API Manager que centralitza la publicació i consum de Serveis en entorns de desenvolupament i pre-producció.



Per a entorns productius es disposa de 2 instàncies d'API Manager separades per a donar Serveis a l'entorn corporatiu intern i a l'entorn d'internet.

Estàndards de Desplegament

Se seguiran els procediments de posada en producció establerts per l'IMI.

Serveis transversals

L'IMI disposa d'un conjunt de serveis que es poden accedir des de qualsevol plataforma. Són els que anomenem Serveis transversals. L'adjudicatari està obligat a la utilització d'aquests serveis transversals pel desenvolupament dels productes objecte d'aquest plec que els necessitin.

Tots aquests serveis estan exposats i s'han de consumir via API manager. La forma d'utilitzar aquests serveis serà la que l'IMI determini.

Els serveis transversals més destacats de l'IMI són aquests:

- Autenticació i autorització.
- GEO codificació.
- Registre d'activitats i tràmits.
- Auditoria de dades afectades per LOPDGDD.
- Generació de reports.
- Model d'Informació de Base (MIB).
- Registre d'entrada.
- Plataforma d'interoperabilitat.
- Signatura electrònica.
- Còpia autèntica i impressió segura.



- Foliat d'expedient.
- Sistema d'impressió i notificació (SICON).
- Planificador de processos batch (UC4)
- Publicació d'edictes (TEU)
- Publicació de Decrets electrònics (eDecrets)
- Plataforma de notificació electrònica
- Sistema de gestió de plantilles (pdfgestor)

El llistat complet de serveis transversals és més extens. Per a cada plataforma de desenvolupament existeix un conjunt de serveis agrupats de la següent manera:

- Propòsit general.
- Presentació.
- Integració.
- Negoci.

L'IMI proporcionarà a l'adjudicatari el llistat complet de serveis transversals. La utilització d'aquests serveis transversals per part de l'adjudicatari ha de ser màxima.

Durant la fase d'anàlisi de necessitats l'adjudicatari col·laborarà en l'avaluació de la idoneïtat de cada servei i les particularitats de la GEU i en les adaptacions que es requereixin.

Sistema de control de versions (GIT)

GitLab és un servei de hosting de repositoris Git, el qual ofereix tota la funcionalitat de Git de control de revisió distribuït i administració de codi de la font (SCM) així com afegint les seves característiques pròpies. A diferència de Git, el qual és estrictament una eina de línia d'ordres, GitLab proporciona una interfície gràfica basada en web i escriptori així com integració del mòbil. També proporciona control d'accés i diverses característiques de col·laboració com bug tracking, administració de tasques, i wikis per cada projecte.

L'IMI utilitza GitLab com a repositori de codi font i de documentació de les aplicacions i serveis objectes d'aquest contracte i serà d'obligatòria utilització i administració per part de l'adjudicatari.

Sistema d'Implantació d'Aplicacions (SIA)

SIA (Sistema de Implantació d'Aplicacions), és el sistema utilitzat per gestionar el desplegament d'aplicacions en l'IMI, aquesta es basa en un catàleg d'aplicacions i un repositori de versions d'aquestes. El sistema gestiona el circuit necessari per desplegar una aplicació des d'entorns de desenvolupament fins als entorns producció, passant pels entorns de pre-producció o 'maqueta'. Aquest circuit de desplegament es manté mitjançant e-mails entre els diferents departaments implicats. Aquest circuit de desplegament es personalitza dependent de la tipologia d'aplicacions.

El sistema tipifica les versions dependent del seu impacte en el desenvolupament i/o desplegament, d'aquesta manera, existeixen tres tipus de versions :



1. Versions. Les versions solen tenir major impacte en el desenvolupament o en el desplegament. Per una versió, el sistema emmagatzema en el repositori tots els arxius que formen la versió.

2. Releases. Les releases solen tenir un impacte mitjà en el desenvolupament o en el desplegament, a diferència de les versions, el sistema només emmagatzema en el repositori els canvis produïts des de la darrera implantació.

3. PTF(s). Les PTF(s) només impliquen petits canvis en el desenvolupament, igual que les releases, només s'emmagatzemen en el repositori els canvis produïts des de la darrera implantació.

El Workflow té petites diferències depenent del tipus de versió que s'està implantant.

Altres punts importants a destacar és l'àmbit de les versions. Es contemplen dos àmbits, un àmbit de producció, el normalment utilitzat i un àmbit de Test o proves, les versions en aquest àmbit estan ubicades en diferents directoris i no es solapen amb les versions de producció.

L'adjudicatari haurà de realitzar els desplegaments en els entorns local i d'integració utilitzant les eines que disposa l'IMI: entorns de desenvolupament ELD o RAD, i sistema de deploys per lots.

L'adjudicatari serà el responsable de realitzar les peticions de traspàs i les validacions del seu correcte funcionament. Caldrà fer servir aquest programa per tal de fer el traspàs de l'aplicació al personal responsable de l'IMI. La responsabilitat de traspassar l'aplicació a Producció és de l'IMI.

Sistema d'Implantació d'Aplicacions (SIDECAR)

SIDECAR (Sistema de Desplegament Continu d'Aplicacions) és el nou sistema utilitzat per automatitzar les operacions del cicle de vida de les aplicacions i dels canvis d'entorn (veure apartat Entorns). Està basat en els processos d'Integració Continua i Desplegament Continu (CI/CD), peces bàsiques del paradigma DevOps.

Aquest sistema és totalment automàtic, començant amb una modificació al codi font al repositori i acabant amb el desplegament a l'entorn de pre-producció (o producció) si totes les comprovacions funcionals i tècniques tenen èxit. El Equip Scrum complet, amb el consens d'arquitectura i Operacions, decidirà si treballarà amb model de "Continuous Delivery" (automatització fins pre-producció) o "Continuous Deployment" (automatització fins producció).

Les funcionalitats bàsiques d'aquest sistema són:

1. Automatitzar el procés de construcció i desplegament
2. Donar suport als processos de gestió del canvi i de la configuració de la SMO integrant-se amb les seves eines (p.e. EasyVista)



3. Donar informació de traçabilitat dels desplegaments per detectar errors
4. Permetre la tornada enrere (rollback) en el cas d'errors

L'adjudicatari, en el moment de començar el projecte, haurà de confirmar la disponibilitat del sistema SIDECAR per a l'aplicació(ons) objecte del contracte. En cas contrari haurà d'utilitzar el sistema que indiqui el departament d'arquitectura.

Planificació de Tasques en Entorns Productius

L'IMI disposa d'UC4 com a planificador corporatiu. L'IMI decidirà en el seu moment quin dels planificadors ha de fer-se servir en cada cas i serà responsable de l'adjudicatari fer les adaptacions necessàries per utilitzar el que correspongui.

Tot procés batch s'ha poder cancel·lar i re-arrencar sense que requereixi cap més intervenció. També cal que s'ajusti a la finestra del batch per evitar que afecti al treball online de l'usuari.

La construcció de processos batch UC4 en desenvolupament i el seu desplegament a Integració i Producció es sol·licitaran a través del procediment estàndard de Gestió del Canvi, i el Control de Versions s'ajustarà al circuit d'entrega de programari utilitzant el sistema que l'IMI determini per aquesta tasca.

4.5.4. Infraestructura necessària per a la prestació del servei

Per al cas dels ordinadors de sobretaula i equips portàtils, el prestatari estarà obligat a configurar la maquinària d'acord amb els requeriments que els equips tècnics de l'IMI indiquin en cada ocasió. El programari de base i d'usuari haurà de complir l'estàndard corporatiu propi de l'Ajuntament de Barcelona, de manera que el proveïdor adjudicatari estarà obligat a proveir-se d'aquest de forma prèvia.

El programari estàndard no es podrà modificar per causes pròpies del material aportat per el proveïdor adjudicatari, i en cas de que existeixi incompatibilitat entre programari i maquinari, el prestatari estarà obligat a proveir un equip homologat per l'IMI per tal de poder treballar amb l'estàndard corporatiu. Els equips homologats seran comunicats per l'IMI a petició del prestatari, que haurà d'informar de les característiques dels equipaments abans de connectar-los a la xarxa corporativa municipal.

En cas de que la prestació del servei s'ubiqui a les instal·lacions del proveïdor adjudicatari, la connexió amb l'IMI es portarà a terme mitjançant una connexió LAN-to-LAN i la instal·lació d'un software a les estacions del client.

Les llicències de software necessàries per desenvolupar el servei correran a càrrec de l'adjudicatari.

Connexió LAN-to-LAN

La connexió LAN-to-LAN entre l'empresa adjudicatària i l'IMI es podrà realitzar a través d'Internet (VPN) o mitjans de comunicació privats (ex: fibra òptica propietària).



En cas de que es realitzi a través de mitjans de comunicació privats, s'haurà de garantir que la informació viatgi correctament xifrada.

En cas de que es realitzi a través de Internet (VPN), serà responsabilitat de l'adjudicatari:

- La contractació i manteniment del seu accés a Internet
- La disposició d'un ample de banda suficient per a garantir la prestació del servei
- La disposició d'un equip que suporti aquest tipus de connexions

A més a més, el proveïdor adjudicatari haurà de disposar del personal tècnic necessari per a la correcta configuració dels equips que acaben el circuit VPN del seu costat i dels seus sistemes de seguretat i translació d'adreces IP. L'IMI col·laborarà en la seva implantació facilitant els paràmetres de configuració i el certificat per a l'equip que acaba el circuit.

De forma opcional, l'IMI podrà oferir un model de configuració tipus si aquest equip final es tracta d'un Router Cisco de la sèrie 800. En cas de dificultats per a establir aquest circuit, l'IMI es reserva el dret de comprovar amb equips de la seva propietat, la causa del problema amb l'objectiu de determinar responsabilitats en la resolució de qualsevol incidència.

Software a les estacions clients

Per tal de poder executar les tasques de manteniment recurrent, caldrà realitzar la instal·lació d'un Software a les estacions del client (sobre plataformes Windows o GNU/Linux). Aquest permetrà accedir a unes màquines de desenvolupament remot que estaran a la seu de l'IMI. És responsabilitat de l'adjudicatari la instal·lació, el seu manteniment, així com disposar dels equips que suportin el Software necessari a instal·lar a les màquines del proveïdor adjudicatari.

Firewall

Serà necessari configurar el Firewall amb les opcions estàndard que indicarà l'IMI. L'accés a la màquina o màquines de desenvolupament assignades es farà mitjançant un o més noms DNS que l'IMI subministrarà. Per a la resolució d'aquests noms cap a una adreça IP també es facilitarà l'adreça d'un servidor DNS de l'IMI capaç de resoldre correctament els noms d'estació. És responsabilitat de l'adjudicatari configurar les estacions o els servidors DNS interns perquè les peticions puguin arribar fins als servidors de l'IMI.

Cada estació de desenvolupament només admet una connexió remota. És responsabilitat del client garantir que cada usuari utilitzi una màquina diferent de les que l'IMI els ha assignat.

Les estacions de desenvolupament estan preparades per a permetre la impressió. Si es requereix algun model no reconegut, caldrà notificar-ho a l'IMI perquè s'afegeixin els *drivers* necessaris. Per poder utilitzar la impressió des de sistemes externs (Host Print o Paris) cal que les impressores tinguin assignada una IP del rang subministrat per l'IMI.

S'ofereix la possibilitat de transferir fitxers entre l'estació de desenvolupament i la de l'usuari, però es recomana fer-ho amb moderació degut a l'alta utilització d'ample de banda que requereix.



4.5.5. Components de software lliure

L'IMI advoca per reduir el nombre de components de software llicenciables, i recomana per tant l'ús de components *Open Source*.

Les solucions, sistemes, processos, metodologies que es defineixin hauran d'estar alineats, ser coherents amb les estratègies TIC de l'Ajuntament, que es poden concretar entre altres en:

- Transparència i participació
- Obertura al ciutadà.
- Agilitat i disseny centrat en l'experiència d'usuari
- Us prioritari de Programari Lliure.
- Compartició i creació de solucions de forma col·laborativa amb comunitats i altres administracions.
- Interoperabilitat
- Dades obertes
- Aplicació de estàndards oficials oberts i lliures, especialment en formats de dades i protocols

En tot el que es refereixi a la definició de programari lliure i estàndards oberts lliures s'aplicarà les definicions de la Open Source Initiative (<https://opensource.org/>).

En concret, respecte a l'ús de programari lliure, s'haurà de prioritzar solucions de codi obert, o la construcció de noves solucions que es lliuraran mitjançant llicències obertes.

En els casos en que no es pugui construir la solució totalment amb mòduls de programari lliure o solucions noves a mida, s'intentarà dissenyar la solució de forma que contempli el màxim de peces o mòduls lliures.

4.6. Facturació

En la facturació del contracte s'utilitzaran les tarifes mitjanes de cada servei de contracte (manteniment correctiu, manteniment recurrent, evolutius recurrents i serveis transversals de manteniment) i de talles de webs, servidors i emmagatzematge (aprovisionament infraestructura) més el consumit de programari com a servei i de llicències.

Càlcul de les tarifes mitjanes: Cada servei de contracte que involucra hores de treball (manteniment correctiu, manteniment recurrent, evolutius identificats, evolutiu recurrent i serveis transversals de manteniment), està compost de diferents perfils i d'una dedicació prevista de cada un d'ells. A partir de la oferta de preus/perfil de cada licitador, se li aplica la dedicació promig de cada perfil per obtenir un preu mitjà per a cada servei.



Donat que els serveis de manteniment correctiu i recurrent són tots dos variables, són també intercanviables a nivell de pressupost. Al llarg de l'any si un dels dos serveis excedeix les previsions aquestes es poden compensar per defecte de l'altre, sense alterar l'import econòmic anual de la suma de tots dos serveis.

Això permet que si un any, per alguna circumstància excepcional, s'incrementa el manteniment correctiu, aquest es pugui cobrir a costa de manteniment recurrent. De la mateixa manera si es fan millores i adaptacions que redueixen el manteniment correctiu, que aquest es pugui utilitzar per abordar més manteniment recurrent.

L'IMI en Comitè de Direcció podrà plantejar una revisió de les previsions de la Línia Base dels serveis del contracte en base a prioritats i identificació de necessitats de la Gerència o del propi IMI. L'adjudicatari haurà d'ajustar els equips i distribucions previstes el més aviat possible i en un període d'1 mes com a màxim.

El primer termini de facturació serà des del dia d'inici de la prestació de cada servei-aplicació fins al darrer dia del mes que correspongui. S'haurà de presentar una factura mensual amb el detall dels serveis d'aplicació que estiguin afectats.

4.6.1. Servei de manteniment correctiu

La facturació del servei de manteniment correctiu serà mensual, a mes vençut i de tipus variable.

L'import total resultarà del nombre d'hores totals (total d'hores dels tiquets registrats com tancats i cancel·lats a l'eina de ticketing, no corresponents a garantia, del mes anterior) multiplicat pel preu per hora del servei de contracte de manteniment correctiu de l'adjudicatari.

En el detall de la factura hi haurà de constar la relació de serveis realitzats, així com l'aplicació de les reduccions d'import corresponents per incompliment dels ANS.

4.6.2. Servei de manteniment recurrent

La facturació del servei de desenvolupament de manteniment recurrent serà variable i es realitzarà a mes vençut segons les validacions realitzades per l'IMI als comitès de seguiment i direcció.

L'import dels manteniments recurrents es calcularà en la fase d'avaluació de necessitats realitzada pel proveïdor adjudicatari i sota acceptació de l'IMI. Per tant, l'import a facturar del manteniment recurrent correspondrà a l'estimació realitzada pel proveïdor i aprovada per l'IMI.

Un cop realitzats els treballs validats i transportats a l'entorn productiu, el Comitè de Seguiment serà l'encarregat de validar i acceptar els treballs realitzats i d'autoritzar la facturació dels mateixos. En cas que el Comitè de Seguiment no autoritzés l'emissió de la factura mensual corresponent, els treballs no podran ser facturats fins a la seva aprovació.



Cada mes es facturaran els treballs enregistrats a l'eina de ticketing amb estat tancat i data de tancament del mes anterior.

Els tiquets de manteniment recurrent cancel·lats es passaran a "Serveis Transversals de Manteniment – Suport tècnic" i l'esforç imputat fins aleshores en concepte de valoració, comptarà com a part dels "Serveis Transversals de Manteniment".

Els tiquets de manteniment recurrent cancel·lats que no hagin estat demanats per l'IMI es passaran a estat facturat, però les hores imputades no seran facturades.

En el detall de la factura haurà de constar la relació de serveis realitzats per a cada servei d'aplicació, així com l'aplicació de les penalitzacions corresponents, si fos el cas, a aplicar per incompliment dels ANS del servei.

4.6.3. Servei d'evolutius recurrents

La facturació del servei de desenvolupament d'evolutius recurrents serà variable i es realitzarà a mes vençut segons les validacions realitzades per l'IMI als comitès de seguiment i direcció.

L'import dels evolutius recurrents es calcularà en la fase d'avaluació de necessitats realitzada pel proveïdor adjudicatari i sota acceptació de l'IMI. Per tant, l'import a facturar del manteniment recurrent correspondrà a l'estimació realitzada pel proveïdor i aprovada per l'IMI.

Un cop realitzats els treballs validats i transportats a l'entorn productiu, el Comitè de Seguiment serà l'encarregat de validar i acceptar els treballs realitzats i d'autoritzar la facturació dels mateixos. En cas que el Comitè de Seguiment no autoritzés l'emissió de la factura mensual corresponent, els treballs no podran ser facturats fins a la seva aprovació. Cada mes es facturaran els treballs enregistrats a l'eina de ticketing amb estat tancat i data de tancament del mes anterior.

Els tiquets d'evolutius recurrent cancel·lats que no hagin estat demanats per l'IMI es passaran a estat facturat, però les hores imputades no seran facturades.

En el detall de la factura haurà de constar la relació de serveis realitzats per a cada servei d'aplicació, així com l'aplicació de les penalitzacions corresponents, si fos el cas, a aplicar per incompliment dels ANS del servei.

4.6.4. Serveis Transversals de Manteniment

La facturació dels Serveis Transversals de Manteniment serà **fix més variable, mensual i a mes vençut**.

L'import **fix** dels Serveis Transversals de Manteniment a facturar mensualment serà el resultat de dividir el preu anual dels Serveis Transversals de Manteniment ofert per



l'adjudicatari i signat en el contracte, entre els mesos efectius de l'any. L'IMI podrà aplicar una ponderació en funció dels dies laborables del mes, els festius o la previsió de vacances.

L'import **variable** vindrà donat per l'import assignat al subservei de:

- Llicències i productes, l'import mensual dels quals pot ser variable en funció de les altes i baixes dels propis productes.

En el detall de la factura haurà de constar la relació de serveis realitzats, així com l'aplicació de les penalitzacions corresponents, si fos el cas, a aplicar per incompliment dels ANS del servei.

El primer termini de facturació serà des del dia d'inici de la prestació de cada servei d'aplicació fins al darrer dia del mes que correspongui. S'haurà de presentar una factura mensual amb el detall dels serveis d'aplicació que estiguin afectats.

4.6.5. Servei d'aprovisionament d'infraestructura

La facturació del servei d'aprovisionament d'infraestructura serà **mensual, a mes vençut** i de tipus **variable**. Es relacionarà el **total d'elements de cada talla** que han estat actius durant el mes corresponent, i l'import total resultarà d'aplicar el preu per talla corresponent (ofert durant la licitació per l'adjudicatari) a cadascun dels totals d'elements per talla.

- El **total d'elements de cada talla** vindrà determinat per la relació d'elements d'infraestructura que han estat actius durant més de set dies durant en el transcurs del mes anterior. Caldrà agrupar-los per cadascuna de les talles, i sumar quants elements n'hi ha de cadascuna.
- El **preu per talla** (de cada tipus) del servei d'aprovisionament d'infraestructura serà el preu ofert per l'adjudicatari en el procés de licitació i signat en el contracte del servei.

A banda, el programari com a servei es factura segons el consumit, sumant tots els serveis proporcionats.

En el detall de la factura haurà de constar la relació d'elements facturables, agrupats per talla, indicant el total d'elements de cada talla, així com l'aplicació de les reduccions d'import corresponents per aplicació dels ANS (penalitzacions).

En el capítol "14.3 volumetria i dades: servei d'aprovisionament infraestructura", es detalla els requeriments de cada talla, i el volum estimat d'elements de cada talla que es traspasaran a l'inici del servei.

4.6.6. Transició: Subcontractació del servei de "La Mercè"

Es requereix subcontractar el servei "La Mercè" el primer any (2024), donat que per raons tècniques i estratègiques es considera que té molt risc traspasar aquest servei el primer any de contracte.



El primer any (2024) l'adjudicatari l'haurà de subcontractar a una empresa donada que porta la seva administració actualment, i a partir del segon any (2025) ja estarà inclosa dins la infraestructura de Webs com un web de talla "Web CMS Estratègica", o bé si requereix infraestructura dedicada, com un "Servidor Virtual dedicat". El segon any, les hores de gestió i suport especials de la campanya es gestionaran com un recurrent normal dins el contracte.

L'Institut imposa al contractista l'obligació de subcontractar amb tercers no vinculats a ell, aquelles parts de la prestació que es concreten i quantifiquen en el pressupost del contracte corresponents a:

- **Servei "Suport Web La Mercè"** (només per l'edició 2024), **per un import total de 8.735,00 € (iva exclòs) + 1.834,35 € (d'IVA) = 10.569,35 € (IVA inclòs)**, per gaudir d'una substantivitat pròpia que el fa susceptible d'execució separada, en haver de ser realitzades per una empresa que compta amb una determinada habilitació professional i experiència adequada per fer-la.
- Donada la concurrència del traspàs del present contracte amb la publicació de la campanya de La Mercè, és un risc gran fer el traspàs d'aquest servei a una nova empresa, donat que aquest web requereix d'un coneixement profund de l'arquitectura existent, de les aplicacions que hi donen servei, de les integracions especials amb l'IMI i d'un operatiu 24x7 especial per poder donar el servei amb garanties.
- L'empresa **Advanced Programming Solutions, S.L. (CIF ESB57608960)** és l'única empresa que compta amb la qualificació i l'experiència adequada per executar-ho durant la primera campanya del setembre del 2024, i, el personal encarregat d'executar els requeriments concrets d'aquest servei d'aplicació del contracte, ja que és l'únic proveïdor que disposa del coneixement tècnic i funcional havent-ne estat l'empresa que durant els darrers 4 anys n'ha modificat el programari de gestió i manteniment dels sistemes d'informació.

En cas de resultar l'adjudicatari d'aquest contracte la mateixa empresa que la que du l'administració de la mercè, no caldrà fer la subcontractació, i l'import íntegre quedarà en el contracte a fi de realitzar el servei de manera normal dins el contracte, facturant per talles i recurrent com ja està previst.

5. MODEL DE PRESTACIÓ DEL SERVEI

5.1. Relació de rols IMI/adjudicatari



Per assegurar el correcte desenvolupament dels serveis i garantir la coordinació entre l'IMI i l'adjudicatari, es requeriran a nivell de gestió, com a mínim, els següents perfils:

Perfil IMI	Perfil Adjudicatari
Responsable del Contracte	Cap de projecte/Responsable del Servei
Responsables de Serveis	Arquitecte Responsable seguretat Programador de sistemes Programador PHP Full Stack Developer en PYTHON Arquitecte PYTHON Atenció usuaris

5.1.1. Perfils IMI

Responsable de contracte:

- Màxim responsable del contracte.
- S'encarrega d'assegurar el compliment dels terminis acordats, així com la qualitat i l'adequació dels serveis objecte d'aquest contracte i l'execució del projecte segons la metodologia i els estàndards de l'IMI.
- Determinarà la relació entre l'Ajuntament, l'IMI, i l'adjudicatari (responsables de servei i altres membres de l'equip de l'adjudicatari).

Responsable de servei d'aplicacions:

- Persones responsables dels serveis objecte d'aquest contracte.
- Coordinaran les sessions de revisions i validacions funcionals amb l'usuari/la usuària i participarà en les sessions d'acceptació dels sistemes desenvolupats per l'empresa adjudicatària.
- Com a responsables tècnic dels serveis objecte del contracte, supervisaran, controlaran i asseguraran l'adequació dels requisits tècnics necessaris per a l'execució dels serveis.
- En cas de necessitat, contactaran i coordinaran els/les interlocutors/es de l'IMI per a les diferents disciplines del contracte:
 - Presa de requisits
 - Arquitectura
 - Implantació
 - Proves
 - Desplegament



- Operacions
- Seguretat
- Telecomunicacions
- Informació Territorial
- Projectes

5.1.2. Perfils adjudicatari

L'adjudicatari proposarà un equip de treball adequat per a l'execució dels serveis. L'IMI estima que l'experiència/coneixements mínims requerits pels perfils necessaris que ha d'aportar l'adjudicatari per a la prestació dels serveis d'aquest contracte són:

Perfil	Experiència i Coneixement
Cap de projecte / Responsable del Servei	<p>Funcions:</p> <p>Màxim responsable del contracte. S'encarrega d'assegurar el compliment dels terminis acordats, així com la qualitat i l'adequació dels serveis objecte d'aquest contracte, el reporting, l'staffing de recursos i l'execució del contracte segons la metodologia i els estàndards de l'IMI. L'interlocutor únic entre l'adjudicatari i l'IMI per a tots els temes relacionats amb la gestió i execució del contracte.</p> <p>Gestiona el projecte, els recursos humans assignats, i vetlla per la qualitat del servei. Convoca els comitès. Interlocutor principal amb l'IMI.</p> <ul style="list-style-type: none">• Experiència i formació mínima requerides: mínim 3 anys en projectes tecnològics• Experiència mínima de 3 anys en l'àmbit de la consultoria estratègica i/o projectes de transformació organitzativa.• Experiència mínima de 3 anys com a Cap de projecte o responsable de servei amb Administració Pública o Privada . <p>Més les responsabilitats incloses a l'apartat "11.10 gestió del personal"</p>
Arquitecte	<p>Funcions:</p> <p>Dissenya la infraestructura, implementa l'automatització, marca les directrius tecnològiques, assegura el rendiment, la robustesa, l'escalabilitat de la plataforma.</p>



	<p>Experiència i formació mínima requerides:</p> <ul style="list-style-type: none"> • Experiència professional: mínim 3 anys en projectes tecnològics. • Haver participat en 3 projectes d'administració d'aplicatius LAMP (Linux / Apache / MySQL / PHP). • Orientat a la gestió de la Infraestructura com a Codi (IaC): Haver participat en mínim de 3 projectes de desplegament amb SALTstack. • Haver participat en un mínim d'1 projecte de desplegament DevOps amb AWS • Coneixements bàsics: <ul style="list-style-type: none"> • Gestió de contenidors: Docker, Kubernetes • Bases de dades: MySQL, Postgresql, Aurora • Sistema operatiu: Linux (Debian/Ubuntu) • Coneixements complementaris (es requereix <u>cobrir almenys un 60%</u> dels mateixos): <ul style="list-style-type: none"> • Cloud públic: DigitalOcean, AWS (amb certificació), GCE, • Infraestructura com a Codi: SALTstack, Packer, Terraform, • Servidors Web: Nginx, Apache, PHP FPM, • Sistemes de memòria cau http: Varnish, CDNs - Cloudfront, • Sistemes de memòria cau: Redis / Memcache • Llenguatges / frameworks desenvolupament: Python / Django / Flask / PHP / Bash • Gestió de versions: GIT, GitLab, pipelines • Gestió d'alta disponibilitat i clusters: Corosync + Pacemaker, HAProxy • Monitorització: Nagios / Checkmk / Telegraf - Influx - Grafana / Cloudwatch • Còpies de seguretat: BareOS • Gestió de traces d'error: Sentry • Gestió d'imatges: Thumbor • Coneixement de protocols de xarxa: HTTP, TLS, TCP/IP, ICMP, DNS, SFTP, SSH, IPSEC
Responsable seguretat	<p>Funcions:</p> <p>Revisa i complementa les guies de bastionat, vetlla per la seguretat, desenvolupa plans de contingència, fa la interlocució amb el departament de seguretat de l'IMI. En concret:</p> <ul style="list-style-type: none"> • i) Actuar d'interlocutor únic per a tots els aspectes de seguretat del contracte.



Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

	<ul style="list-style-type: none"> • ii) 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. • iii) 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 pel l'IMI. • iv) 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 (com a mínim en el moment de la incorporació a l'equip). • v) Assegurar que tot el personal del proveïdor que hagi de tractar dades o sistemes de tractament de dades de nivell sensible o superior signin un Acord de Confidencialitat Individual. L'IMI podrà auditar aquest aspecte. • vi) Informar al seu personal qualsevol obligació a la que l'empresa estigui sotmesa per contracte, formar al seu personal en la política 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. • vii) Mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en que 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. També anotarà la data de revocació dels accessos quan s'hagi fet. <p>Més les responsabilitats incloses a l'apartat "11.1 Responsable de seguretat".</p> <ul style="list-style-type: none"> • Experiència i formació mínima requerides: Haver participat en 3 projectes d'administració d'aplicatius LAMP (Linux / Apache / MySQL / PHP) • Haver participat en 3 projectes com a responsable de seguretat. • Coneixements bàsics: AWS Firewall, AWS Security Groups
Programador de	Funcions:



sistemes	<p>Administra la infraestructura, aplica les guies de bastonat, implementa nous sistemes, realitza proves de qualitat del sistema, revisa com a mínim diàriament la monitorització i traves del sistema per detectar punts de millora realitza les funcions de DevOps.</p> <p>Experiència i formació mínima requerides:</p> <ul style="list-style-type: none">• Mínim de 3 anys d'experiència professional en aquest rol• Haver participat en 3 projectes d'administració d'aplicatius LAMP (Linux / Apache / MySQL / PHP).• Orientat a la gestió de la Infraestructura com a Codi (IaC): Haver participat en mínim de 3 projecte de desplegament amb SALTstack• Haver participat en un mínim d'1 projecte de desplegament DevOps amb AWS
Programador PHP	<p>Funcions:</p> <p>Realitza el manteniment dels webs Drupal i Wordpress, en quant a incidències de seguretat, conflictes de configuració en quant a la plataforma, aplicació de canvis massius a tots els webs gestionats al contracte (ex. Conversió de http a https, inclusió de Redis per accelerar el rendiment, pujades de versió davant la publicació de vulnerabilitats greus).</p> <p>Experiència i formació mínima requerides:</p> <ul style="list-style-type: none">• Haver participat en 3 projectes d'administració d'aplicatius LAMP (Linux / Apache / MySQL / PHP)• Experiència en manteniment de seguretat en Drupal/Wordpress d'almenys 1 any• Experiència en desenvolupament i execució de proves unitàries en almenys 3 projectes.
Full Stack Developer en PYTHON	<p>Funcions:</p> <p>Manté aplicacions Python/Django, incorporant noves funcionalitats o solucionant incidències. Assumeix també el rol de desenvolupador React.</p> <p>Experiència i formació mínima requerides:</p> <ul style="list-style-type: none">• Mínim de 3 anys d'experiència professional en aquest rol• Assumeix també el rol de Desenvolupador React: Mínim de 2 anys d'experiència professional en React (el Frontal de Sygox està construït amb React
Arquitecte PYTHON	<p>Funcions:</p> <p>Identifica necessitats i requeriments, dissenya sistemes d'informació, avalua alternatives de disseny, marca les</p>



	<p>directrius. Fa el manteniment de les Eines de govern, construïdes amb Python</p> <p>Experiència i formació mínima requerides:</p> <ul style="list-style-type: none">• Mínim de 3 anys d'experiència professional en aquest rol• Experiència en desenvolupament i execució de proves unitàries en almenys 3 projectes.
Atenció usuaris	<p>Funcions:</p> <p>Atén les peticions i els avisos, via les eines de suport, o telefòniques, aclareix dubtes de les peticions, vetlla perquè l'estat de les peticions estigui puntualment informat. Organitza els repositoris de documentació del projecte (al Wiki del Gitlab de l'Ajuntament).</p> <p>Experiència i formació mínima requerides:</p> <ul style="list-style-type: none">• Experiència: Mínim d'1 any d'experiència professional en projectes tecnològics

Certificacions de l'Equip:

- L'equip tècnic vinculat al servei ha de tenir com a mínim:
 - Per a l'Arquitecte assignat a l'equip:
 - Certificació AWS "Certified Solutions Architect - Associate" o superior (Referència: <https://aws.amazon.com/certification/certified-solutions-architect-associate/>)
 - Per 1 persona assignada a l'equip:
 - certificació de **Scrum Master** (Professional Scrum Master I (PSM I) de Scrum.org (o superior)
Ref: <https://www.scrum.org/courses/professional-scrum-master-training>
o bé
Certified ScrumMaster (CSM) de Scrum Alliance (o superior).
Ref: <https://www.scrumalliance.org/get-certified/scrum-master-track/certified-scrummaster>

Aquests perfils poden ser compartits per una mateixa persona o bé repartits entre diverses persones de l'equip, indicant per cada una d'elles el percentatge de dedicació, a excepció dels següents perfils dels quals es requereixen persones amb dedicació exclusiva a un únic perfil (una mateixa persona no comparteixi més d'un perfil):

- Cap de projecte / Responsable del Servei
- Arquitecte
- Responsable seguretat



Els licitadors, mitjançant una declaració responsable en la forma que s'indica en el plec de clàusules administratives particulars, acreditaran que disposen de l'equip de treball amb l'experiència professional exigida i amb coneixements dels entorns tecnològics requerits i que el posaran a disposició del contracte, en cas de resultar adjudicatari. Aquests coneixements dels entorns tecnològics han de ser justificats amb els certificats dels cursos exigits en el punt de capacitat, aptitud i solvència dels licitadors del document de clàusules administratives. És a dir, els certificats aportats per acreditar la solvència tècnica han d'estar expedits a les persones assignades a l'equip de treball de l'adjudicatari per aquest contracte.

L'IMI es reserva el dret de verificar (amb entrevistes, consultes de les referències, exàmens de coneixements o amb altres vies) les capacitats del personal que participa en el contracte en qualsevol moment i rebutjar-lo en cas que no compleixin amb els requisits exigits. Les despeses que es derivin com a conseqüència de canvis en l'equip de contracte aniran a càrrec de l'adjudicatari.

Els licitadors hauran d'incloure en la seva oferta, un esquema de l'equip del treball indicant el percentatge de dedicació i la seva organització.

Per temes puntuals es podrà exigir que membres de l'equip de treball treballin presencialment a les instal·lacions que l'IMI determini (veure apartat 4.1).

L'adjudicatari haurà de mantenir l'equip de treball adscrit al contracte durant tota la seva vigència. En cas que s'hagi de produir la substitució d'algun membre de l'equip, l'adjudicatari ho haurà de comunicar en el Comitè de Direcció del servei i la substitució s'haurà de fer per un perfil que com a mínim tingui les mateixes característiques professionals i tècniques; en cas contrari i sense el consentiment de l'IMI aquest fet serà susceptible de sanció.

Les substitucions que no siguin motivades per causa major, és a dir que no depengui de qualsevol de les parts, restaran prohibides. Només seran possibles si aquesta és validada amb el/la responsable del contracte i en tot cas hauran de ser planificades per minimitzar l'afectació al servei. En cas de causa major caldrà justificar-la i acreditar-la convenientment.

En el cas de substitució d'algun membre de l'equip, s'haurà de seguir el següent procediment:

- Comunicació per escrit al responsable del contracte de l'IMI amb un preavis mínim de 10 dies laborables (veure ANS Pre Subs a l'apartat 8).
- Comunicació per escrit a l'IMI (departament "Suport DSV") del canvi del perfil sortint i el perfil entrant, detallant per aquest últim, el compliment dels requeriments d'experiència detallats al plec de prescripcions tècniques i a l'oferta del proveïdor, en el cas que hi hagi presentat millores.
- El departament "Suport DSV" de l'IMI presentarà la informació al responsable del contracte de l'IMI per a la seva validació:
 - En el cas de ser positiva l'adjudicatari comunicarà la substitució a Administració de l'IMI per obtenir el vistiplau per realitzar la substitució i incorporar el nou perfil.



- En el cas de ser negativa l'adjudicatari haurà de presentar un nou candidat en 5 dies laborables.

El nou treballador/a haurà d'incorporar-se com a mínim 5 dies laborables abans de la sortida del treballador/a substituït.

A més s'exigirà com a **període no facturable del nou perfil** el següent:

- Un període de formació, de mínim tres setmanes, a càrrec de l'adjudicatari, pel nou membre que s'incorpori a l'execució del contracte,
- Un període de coexistència d'una setmana, entre la persona que causa baixa i la persona que s'incorpora.

En relació a aquest període no facturable tant de l'equip existent com pel nou membre que s'incorpora es durà a terme el que es detalla a l'apartat 3.2.7. Formació per a noves incorporacions.

Serà responsabilitat de l'adjudicatari confirmar la plena incorporació del perfil a la dinàmica de treball i de la seva bona resposta a les demandes del servei.

L'adjudicatari ha de revisar el nivell de qualitat i aportació realitzada pels seus tècnics i equips, així com l'organització del servei proposant a l'IMI les millores, ajustos i substitucions necessàries per fomentar la millora del servei.

En cas que algun dels perfils del servei no resolgui amb solvència, efectivitat i qualitat les tasques encomanades l'IMI podrà sol·licitar la seva substitució, que l'adjudicatari resoldrà amb el mateix procediment descrit anteriorment i en un període no superior a 2 setmanes, assumint de nou l'adjudicatari els costos associats a aquesta substitució.

En relació a les possibles modificacions del contracte es requereix que l'adjudicatari com a mínim mantingui la piràmide de perfils plantejats. L'IMI podrà determinar peticions concretes que requereixi una estructura de perfils en funció de les necessitats. De la mateixa manera, en cas que el proveïdor proposi una millora econòmica en quant a tarifes, caldrà mantenir com a mínim la distribució de la piràmide de perfils plantejats.

5.2. Model de govern

Per la correcta 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 pels següents comitès:

- Comitè de Seguiment Operatiu
- Comitè Tècnic
- Comitè de Direcció

Excepte que l'IMI comuniqui el contrari, el Cap de Projecte de l'adjudicatari és l'encarregat de fer les convocatòries, amb un mínim de **10 dies laborables d'antelació**, i enviar la documentació necessària als participants com a mínim amb **2 dies laborables d'antelació**



(*), i d'aixecar acta de les reunions. En cas de comitès extraordinaris es convocaran amb un mínim d'un dia d'antelació i no serà necessari enviar la documentació amb anterioritat.

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

(*) Per exemple, **si el comitè comença el dilluns a les 10:00 i acaba a les 11:00 hores**, i l'horari del servei es de dilluns a divendres, de 8:00 a 18:00 hores:

- L'adjudicatari ha d'enviar la documentació necessària als participants **abans de les 10:00 hores del dijous anterior**, si dijous i divendres són dies laborables, si fossin festius, s'avançaria a les 10:00 hores del dimecres anterior si un dels dos és festiu, o al dimarts a les 10:00 hores si els dos fossin festius.
- L'adjudicatari ha d'enviar l'acta **abans de les 11:00 hores del dimecres** després de la reunió. Si dimarts o dimecres fossin festius, es mouria un o dos dies, a abans de les 11:00 hores del dijous o del divendres.

5.2.1. Comitè de Seguiment Operatiu

Es reunirà amb caràcter quinzenal per a cada àrea o grup de serveis o bé amb sessions conjuntes de tots els grups de servei si així ho determina l'IMI, encara que ambdues parts els podran convocar també amb caràcter extraordinari sempre que es consideri necessari.

Inicialment es consideraran dos grups de servei amb comitè de seguiment propi:

- Gestió del manteniment
- Gestió dels evolutius recurrents

En formen part:

- Responsable de servei de l'IMI
- Coordinador del contracte de l'adjudicatari
- Cap de projecte de l'adjudicatari
- Responsable de serveis de l'adjudicatari

Li corresponen al Comitè de Seguiment les funcions de:

- Revisió de les incidències en curs i el seu pas a problema si així es considera per l'IMI.
- Revisió dels problemes en curs.
- Validació i acceptació dels treballs recurrents realitzats.
- Verificació de les proves exhaustives realitzades.
- Resolució dels conflictes que puguin sorgir.
- 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).



- Seguiment de les necessitats de llicències i productes per a la prestació del servei de cada aplicació.
- Verificació ANS i proposta de facturació.
- Sessió prèvia preparatòria del Comitè de Direcció. Es revisa el mateix contingut i es planteja els punts destacats o decisions a traslladar al Comitè de Direcció.
- Totes aquelles que l'hi atribueixi el present plec.

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. A l'inici del contracte es determinarà el detall i contingut de la documentació de seguiment.

5.2.2. Comitè Tècnic

Es reunirà amb caràcter mensual, encara que ambdues parts els podran convocar també amb caràcter extraordinari sempre que es consideri necessari.

En formen part:

- Responsable contracte IMI
- Responsable de servei l'IMI
- Responsable arquitectura IMI i tècnics IMI que consideri
- Cap de projecte de l'adjudicatari
- Arquitecte/a de l'adjudicatari (perfil Arquitecte/a del contracte)

Li corresponen al Comitè Tècnic les funcions de:

- Revisió de temes tècnics del servei.
- Realització de tasques de coordinació amb diferents departaments tècnics relacionats amb el servei.
- Resolució dels conflictes que puguin sorgir.
- Totes aquelles que l'hi atribueixi el present plec.

Li correspon al responsable de l'empresa adjudicatària la preparació de la documentació necessària per a la realització del Comitè Tècnic i aixecar acta dels temes i acords de la reunió. A l'inici del contracte es determinarà el detall i contingut de la documentació de seguiment.

5.2.3. 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 es podrà convocar amb caràcter extraordinari sempre que es consideri necessari. En formen part:

- Director/a de Desenvolupament de l'IMI
- Responsable de contracte de l'IMI
- Responsables de l'IMI



- Coordinador/a del contracte de l'adjudicatari
- Cap de projecte de l'adjudicatari
- Altres assistents requerits (a petició de l'IMI)

Li corresponen al Comitè de Direcció les funcions de:

- Control de l'execució del contracte
- Validació i aprovació de l'emissió de la factura corresponent als treballs realitzats
- Resolució dels conflictes que puguin sorgir en l'execució del contracte
- Revisió de l'estat dels Checkpoints
- Revisió de resultats d'auditories
- Comunicació de substitució de membres de l'equip si s'escau, validació de les característiques tècniques i professionals del substitut i presentació del període de formació i de coexistència
- Aprovar ampliacions/reduccions de contracte
- Verificació de l'acompliment dels ANS i del contracte
- Comunicació de les faltes i penalitzacions i afectació en la propera facturació si s'escau
- 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. L'ordre del dia del comitè haurà d'incloure com a mínim els punts detallats en el punt 3.5.4.1 Reporting i com a primer punt sempre hi constarà els punts o acords de l'anterior acta de seguiment.



6. EINES DEL SERVEI

A continuació es detallen algunes de les eines que s'utilitzen en l'actualitat a l'IMI per a la gestió de nous Desenvolupaments, Manteniments Evolutius i incidències en funció del tipus de contracte que s'estigui executant. L'ús de les mateixes està descrit en ADINET/Metodologia AGILE així com en els diversos procediments vigents a l'IMI. L'IMI es reserva el dret de modificar aquestes eines amb el previ avís suficient perquè els proveïdors puguin adaptar-se a les mateixes.

Les eines esmentades anteriorment tenen les següents característiques:

- **Eina de gestió de peticions:** Aplicació mitjançant la qual es realitzen els registres i posterior seguiment de les peticions de les aplicacions que es troben a l'entorn de Producció.
- **Eina de gestió d'incidències:** Aplicació mitjançant la qual es realitzen els registres i posterior seguiment de les incidències de les aplicacions que es troben a l'entorn de Producció.
- **Eina de ticketing:** Aplicació mitjançant la qual es realitzen els registres i posterior seguiment del cicle de vida de les tasques dels serveis de manteniment i les imputacions dels esforços corresponents.
- **Eina de gestió de requisits:** Aplicació mitjançant la qual es realitza la gestió de requisits i proves.
- **Eines verticals de proves:** Conjunt d'eines Open Source utilitzades per a l'execució de les proves associades a requeriments no funcionals.
- **Eina de gestió del contracte:** Eina de gestió de la demanda, de contractes i de serveis.
- **Eina de reporting de serveis:** Aplicació de gestió dels indicadors, de seguiment dels ANS i dels altres indicadors del contracte.
- **Eina de seguiment de projectes:** Aplicació de gestió dels projectes, de seguiment de fites i checkpoints, riscos i pressupost.
- **Eina de comunicació i treball col·laboratiu:** Plataforma utilitzada per gestionar la comunicació i el treball col·laboratiu de manera centralitzada.
- **Plataforma de formació:** Plataforma utilitzada per gestionar la formació en línia.
- **Eina d'enquestes:** Plataforma que permet la realització d'enquestes i la identificació de les persones que entren.
- **Eina de gestió del coneixement:** Plataforma que permet la gestió del coneixement de manera centralitzada.
- **Eina de control de versions:** Plataforma que permet el versionat del codi de les aplicacions i serveis.
- **Eina de càrrega i migracions**

L'IMI comunicarà a l'adjudicatari a l'inici del contracte la relació concreta d'eines del servei i podrà canviar-les durant l'execució del contracte, informant al corresponent adjudicatari amb una antelació mínima de 30 dies naturals.



7. QUALITAT DELS SERVEIS

7.1. Pla de qualitat

El Pla de Qualitat inclourà tots els requisits definits en el present plec per part de l'IMI.

Els punts que s'indiquen a continuació serà l'índex que, com a mínim, ha d'emplenar l'adjudicatari:

- Gestió de la Configuració: Assegurament que els canvis no afecten els nivells de qualitat del servei.
- Resolució dels problemes relatius a la gestió del servei.
- Control de la traçabilitat del programari i de la documentació.
- Procediments que assegurin que la documentació s'ha actualitzat d'acord amb els canvis o peticions realitzades al llarg del cicle de vida del servei.
- Regles i procediments que garanteixin la millora contínua del servei.
- Revisions internes que assegurin que les aplicacions i els serveis compleixen les metodologies definides ADINET/Metodologia AGILE.
- Mètriques i indicadors.
- Proves d'un servei:
 - Estratègia de proves per servei (nous desenvolupaments, evolutius i incidències)
 - Nivells de proves a realitzar per servei
 - Tipus de proves (funcionals, no funcionals, de regressió, rendiment, revisions de documentació, anàlisi estàtic de codi, etc.)
 - Rols involucrats per part del proveïdor
 - Eines involucrades en la gestió de proves i en la gestió de defectes
- Gestió de les responsabilitats relatives a l'actualització del Pla de Qualitat
- Gestió de riscos que possibiliti una reducció o eliminació dels possibles impactes en el servei

L'adjudicatari haurà d'executar el Pla de Qualitat específic que assegurin la qualitat dels serveis oferts.

7.2. Qualitat del servei

Li correspon a l'adjudicatari establir les mesures que consideri adients per lliurar les tasques del contracte amb els nivells mínims de qualitat que li són exigits.

En aquest sentit, l'IMI exigità l'acompliment dels nivells de servei descrits a l'apartat 8 i obliga a l'ús de les metodologies que l'IMI especifiqui en totes les tasques que executi l'adjudicatari.

Amb auditories aleatòries en el temps que es facin sobre el conjunt de les tasques o en algunes fases d'aquest conjunt tant des de l'òptica tècnica com des de l'òptica d'acompliment de la metodologia, l'IMI procedirà a l'avaluació d'aquesta qualitat comprovant:



1. L'acompliment dels acords de nivell de servei.
2. El rebuig o no acceptació de les tasques determinades en la petició que no hagin acreditat l'entrega del programari i la documentació associada. Sempre, i en tot cas, s'haurà d'entregar com a part del programari i la documentació, un Informe del Resultat de l'execució de les proves, juntament amb el seu enregistrament (possibles opcions: fitxer de resultats generat per una eina de proves, lliurament d'un fitxer log, captura de finestres amb el resultat de les proves,...), i es presentarà a l'equip de l'IMI per a la seva consideració i validació en cas que ho consideri necessari.

7.3. Auditories

L'IMI, en funció del desenvolupament del contracte, podrà realitzar auditories sobre el conjunt del treball des de la vessant de qualitat.

L'auditoria ha de servir per millorar la qualitat del servei entesa com la millora del procediment del manteniment d'aplicacions.

L'auditoria en cas que s'exigeixi ha de complir els següents requisits:

- Periodicitat: A determinar per l'IMI
- Àmbit: La totalitat de les aplicacions
- Serveis a auditar: Tots els serveis inclosos a l'abast del contracte
- Equip: Empresa externa i independent
- Resultat: informe d'auditoria

7.3.1. Objectiu de les Auditories

L'objectiu de les Auditories i Revisions de Qualitat dels Serveis Contractats és proporcionar visibilitat i control a la Direcció de l'IMI, sobre el grau de compliment dels adjudicataris amb els aspectes formals del servei.

Els aspectes més rellevants a verificar des del punt de vista d'Auditoria i que apliquen a qualsevol tasca dels serveis del contracte són:

- Verificació de l'esforç estimat/realitzat.
- Verificació dels anàlisis funcionals, tècnics i d'arquitectura.
- Verificació de la documentació generada.
- Revisió de solució implementada.
- Verificació del compliment del Pla de Qualitat de Servei, de les condicions contractuals i dels procediments de treball establerts.
- Pla de Qualitat del Servei: fent especial èmfasi en els mecanismes d'assegurament de la qualitat proposats per l'adjudicatari per a les seves pròpies activitats (controls, revisions, proves, auditories internes de l'adjudicatari, etc.)
- Condicions contractuals: verificant, entre d'altres aspectes, el compliment dels requisits d'infraestructura (entorns, eines, comunicacions, etc.), requisits de personal i requisits de seguretat inclosos en el contracte.



- Procediments de treball: verificant el compliment del Model Operatiu i els procediments definits per a la prestació del servei (activitats, i lliurables).

Els aspectes més rellevants a verificar des del punt de vista d'una revisió són:

- Revisió del compliment i execució del Pla d'Acció proposat.

7.3.2. Procediment d'Auditoria

L'auditor farà l'anàlisi que consideri necessari i requerirà al proveïdor adjudicatari tota aquella informació que consideri adient.

L'adjudicatari cooperarà en l'auditoria, responent immediatament a les informacions demanades per a l'execució de la mateixa i auxiliant als auditors en allò que considerin necessari.

Tota informació addicional o canvis de conducció d'un procés o com a resultat d'auditoria, serà considerada informació confidencial, segons els termes i condicions del contracte.

La realització de l'auditoria en cap moment no eximirà a l'adjudicatari del compliment dels compromisos derivats de la prestació dels serveis d'acord amb els termes inclosos en aquest Plec.

Els costos dels mitjans emprats per l'adjudicatari associats a les auditories no podran ser repercutits en cap cas a l'IMI.

7.3.3. Resultats de l'Auditoria

L'auditoria es realitzarà mitjançant revisions dels diferents aspectes que es contemplen en aquest plec, en el pla de qualitat del servei, en el grau de compliment de l'ús de la metodologia ADINET/ Metodologia AGILE, formació, model de prestació del servei, així com qualsevol altre pla detallat en aquest plec. L'equip auditor buscarà la conformitat amb els aspectes establerts en aquests documents. Per a cada aspecte revisat existiran quatre possibles valoracions:

- **Conformitat:** si es compleix completament amb el que indiquen aquests documents.
- **No Conformitat Major:** si hi ha evidències d'incompliment de requisits relacionats amb el Cicle de Vida del Desenvolupament i Manteniment, els procediments vigents en el moment d'execució de l'auditoria relatius als serveis d'aquest plec i aspectes de Seguretat que incideixen directament en la prestació del servei (Documentació i Lliurables, Gestió de la Configuració, Traçabilitat, Gestió de Riscos i Problemes, Seguretat Físic-Lògica).
- **No Conformitat Menor:** si hi ha evidències d'incompliment de requisits no relacionats amb el Cicle de Vida del Desenvolupament i Manteniment i els procediments vigents en el moment d'execució de l'auditoria relatius als serveis d'aquest plec que incideixin directament en la qualitat del servei (Rols, equip del servei, Temes Laborals i Subcontractacions, solvència tècnica).



- **Observació:** addicionalment, s'inclouran com "observació" aquells fets identificats que afectin o puguin afectar, segons el parer de l'equip auditor, a la qualitat del servei, però que no suposin un incompliment formal dels compromisos establerts. Les observacions identificades en un informe d'Auditoria podrien derivar a No Conformitats en futures auditories si no s'esmenen.

A la finalització de l'auditoria les parts revisaran les desviacions i / o observacions detectades respecte a l'acordat en el contracte. L'adjudicatari haurà d'executar el Pla d'acció definit en l'auditoria amb:

- Accions per assegurar que les desviacions i / o observacions detectades es corregeixin.
- Identificació de responsables i dates límit per a l'execució de les accions.

Serà responsabilitat de l'adjudicatari la realització de les accions establertes en el Pla d'acció.

7.3.4. Resultats de la Revisió

L'IMI podrà realitzar una revisió de l'execució del Pla d'acció proposat.

El mètode consistirà en la revisió del Pla d'acció de cadascuna de les No Conformitats detectades i també es revisaran algunes de les observacions.

S'avaluarà l'estat de l'acció corresponent i en cas de donar-se com a vàlid es considerarà "tancada la No Conformitat".

7.4. Qualitat de Programari

El conjunt del programari objecte d'aquest plec estarà subjecte als controls de qualitat o verificació de validesa que l'IMI determini. En aquest sentit l'adjudicatari haurà de procedir a realitzar el conjunt de proves funcionals i tècniques que l'IMI determini de manera estàndard per les aplicacions.

Dintre d'aquest conjunt de proves es preveuen les de càrrega, regressió i conceptuals, que es realitzaran utilitzant els mètodes, eines i programari accessori que l'IMI determini, obligant-se l'adjudicatari a la realització i/o col·laboració en la confecció dels scripts corresponents a tal efecte.

8. ACORDS DE NIVELL DE SERVEI (ANS)

Per a la gestió i seguiment dels serveis prestats per a l'adjudicatari, es defineixen una sèrie d'Acords de Nivell de Servei (ANS). Aquests permeten monitoritzar i avaluar la qualitat, i, la gestió dels serveis a través d'indicadors que parametrizen el grau de consecució acordat per a cada servei.



Els indicadors tindran la següent estructura en comú:

- **Indicador:** Codi de l'indicador.
- **Descripció:** Definició de l'indicador i objecte de mesura.
- **Càlcul:** Fórmula per al càlcul de l'indicador.
- **ANS:** Acord de nivell de servei d'aplicació a l'indicador.
- **Descompte factura:** Import a descomptar de la factura mensual en el cas d'incompliment de l'ANS.

El compliment dels ANS ha de ser revisat de manera mensual. En el comitè de direcció s'haurà de realitzar una presentació de l'estat de compliment dels ANS, així com de les desviacions ocorregudes.

Per tal d'assegurar la fiabilitat i l'automatització de l'extracció dels ANS del servei, es requereix l'enviament d'informació des de les diferents eines de registres, segons s'estipula a l'**apartat 6** Eines del servei, a través de les APIS actualitzades dels sistemes de l'IMI, cap a una plataforma web de recollida de les dades. L'IMI es reserva el dret de fer servir un altre sistema per extreure la informació que permeti fer el seguiment del contracte i dels ANS informant al corresponent adjudicatari amb una antelació mínima de 30 dies naturals.

L'adjudicatari enviarà la informació requerida i prèviament pactada amb l'IMI.

8.1. ANS de qualitat operativa del servei

Per tal d'assegurar la correcta aplicació dels ANS, s'ha establert un criteri de **criticitat d'incidència**, diferenciant entre incidències greus i incidències normals:

- Es considera que la incidència és **greu** quan l'aplicació productiva estratègica o una de les seves funcionalitats està indisponible més de 10 minuts i això implica una aturada en l'operativa de funcionament normal.
- Es considera que la incidència és **normal** en la resta de casos de webs productives.
- Per als entorns de desenvolupament, s'entén com a peticions de suport.

Totes les incidències es crearan amb criteri d'incidència normal, i en cas de ser greu, **haurà de ser modificat per l'adjudicatari** en el moment d'anàlisi inicial de la mateixa o per indicació de l'IMI. En el cas d'incidències excepcionals, el responsable del contracte de l'IMI, té la potestat de determinar que la incidència concreta queda fora d'algun dels ANS anteriors.

Pel càlcul dels ANS, es consideren com a hores laborables, les de l'horari base de prestació dels serveis del contracte (veure apartat 4.2.1), o bé de les millores que hagi ofert l'adjudicatari a la seva proposta, durant tot l'any.

Es podran millorar a les ofertes els ANS, veure apartat dels criteris de valoració.



8.1.1. Servei de manteniment correctiu

El càlcul dels següents ANS s'haurà de fer per petició de manteniment correctiu **amb periodicitat mensual** i considerant hores laborables i mes natural.

Indicador	Descripció	Càlcul	Criticat incidència	ANS	Descompte factura
Temps de resolució incidència (Inc Tres)	Temps que transcorre entre la comunicació d'una incidència i la resolució efectiva. No ha de superar el llindar d'hores definit	Inc Tres = Data resolució incidència (*) - data d'entrada incidència	greu	Inc Tres <= 8 hores laborables	Import de les hores treballades a la incidència
			normal	Inc Tres <= 18 hores laborables	Import de les hores treballades a la incidència
Tancament d'incidència (Inc tanc)	Temps que transcorre entre la comunicació d'una incidència i la resolució efectiva. No ha de superar el llindar d'hores definit, que és de 24 hores laborables addicionals sobre el llindar de Tres per a la mateixa criticitat d'aplicació/incidència	Inc tanc = Data resolució incidència (*) - data d'entrada incidència	greu	Inc tanc <= 32 hores laborables	200 € per incidència que incompleixi l'ANS
			normal	Inc tanc <= 42 hores laborables	200 € per incidència que incompleixi l'ANS
Incidència no resolta (Inc no res)	Incidències no resoltes en la data prevista Inc Tanc	Inc no res = Nº incidències que tenen activat l'ANS Inc tanc en la data del comitè i no estan resoltes			200 € per incidència que incompleixi l'ANS (**)
Incidències Pending (Inc Pen)	Nº d'incidències amb estat pending sense justificació i no acordades amb responsable de l'IMI	Inc Pen = nombre d'incidències amb estat pending sense justificació i no acordades amb responsable de l'IMI	normal	Inc tanc <= 0 incidències	200 € per incidència que incompleixi l'ANS
Tancament de problemes (Pr tanc)	Problema resolt i lliurat a l'IMI a la data compromesa.	Pr tanc = Data de lliurament (*) - Data compromesa		Pr tanc <= 0 dies laborables	3.000 € per problema que excedeixi l'ANS

(*) Es considera data de resolució d'incidència o problema quan la incidència/problema està solventada, provada i en disposició de ser transportada a l'entorn pre productiu i tancada quan té l'estat *Closed* a l'eina de tiqueting
() L'ANS "Inc no res" serà d'aplicació mensual fins la resolució de la incidència, és a dir, una mateixa incidència podrà penalitzar en diverses factures mensuals**



8.1.2. Serveis de manteniment recurrent

El càlcul dels següents ANS s'haurà de fer per cada petició de manteniment recurrent **amb periodicitat mensual** i considerant dies laborables.

Indicador	Descripció	Càlcul	ANS	Descompte factura
Anàlisi i planificació de peticions (Plani)	Temps que transcorre entre la sol·licitud de valoració d'una petició de recurrent i el lliurament a l'IMI de la valoració.	Plani = Data de lliurament de la valoració - data sol·licitud de valoració del recurrent.	Plani <= 10 dies laborables	200 € per petició que incompleixi l'ANS
Compliment dates d'entrega (Cde)	Manteniment recurrent realitzat i lliurat a l'IMI a la data compromesa.	Cde = Data de lliurament (*) - Data compromesa	Cde <= 0 dies laborables	10% de l'import estimat de la valoració del recurrent per petició que incompleixi l'ANS

(*) Es considera data de lliurament quan la petició recurrent està realitzada, provada i en disposició de ser transportada a l'entorn productiu

8.1.3. Serveis d'evolutius identificats

El càlcul dels següents ANS s'haurà de fer per evolutiu **amb periodicitat mensual** i considerant dies laborables.

Indicador	Descripció	Càlcul	ANS	Descompte factura
Compliment dates d'entrega (Cdev)	Manteniment evolutiu realitzat i lliurat a l'IMI en un termini inferior a l'ANS	Cdev = Data de lliurament (*) - Data compromesa	Cdev <= 0 dies laborables	6% de l'import estimat de la valoració de l'evolutiu per petició que incompleixi l'ANS

(*) Es considera data de lliurament quan l'evolutiu està realitzat, provat i en disposició de ser transportat a l'entorn productiu

(**) Data compromesa al pla de projecte aprovat al kick-off, o la que escaigui si s'han aprovat en el Comitè de Direcció del contracte canvis de planificació. La planificació actualitzada de cadascun dels evolutius haurà d'estar registrada i actualitzada a l'eina de gestor de projectes i a l'eina de tiqueting del servei de manteniment, per poder mesurar aquest indicador.

8.1.4. Serveis Evolutius Recurrents

El càlcul dels següents ANS s'haurà de fer per cada petició de manteniment recurrent **amb periodicitat mensual** i considerant dies laborables.



Indicador	Descripció	Càlcul	ANS	Descompte factura
Anàlisis i planificació de peticions (Plani)	Temps que transcorre entre la sol·licitud de valoració d'una petició de recurrent i el lliurament a l'IMI de la valoració.	Plani = Data de lliurament de la valoració - data sol·licitud de valoració del recurrent.	Plani <= 10 dies laborables	200 € per petició que incompleixi l'ANS
Compliment dates d'entrega (Cde)	Manteniment recurrent realitzat i lliurat a l'IMI a la data compromesa.	Cde = Data de lliurament (*) - Data compromesa	Cde <= 0 dies laborables	10% de l'import estimat de la valoració del recurrent per petició que incompleixi l'ANS

(* Es considera data de lliurament quan la petició recurrent està realitzada, provada i en disposició de ser transportada a l'entorn productiu

8.1.5. Serveis Transversals de Manteniment

El càlcul dels següents ANS s'haurà de fer per indicador **amb periodicitat mensual** i considerant dies laborables.

Indicador	Descripció	Càlcul	ANS	Descompte factura
Entrega d'actes i documentació (Tdocu)	Retard en l'entrega d'actes i documentació (*)	Tdocu = data d'entrega real de cada document – data prevista d'entrega	Tdocu <=0 dies laborables	200 € per document que excedeixi l'ANS
Temps de gestió de llicències (Tllic)	Temps que transcorre des de que es realitza la petició fins que finalitza la gestió	Tllic = Data de finalització de la gestió - data de sol·licitud	Tllic <=20 dies laborables	500 € per petició de llicència que excedeixi l'ANS
Qualitat dels documents entregats (Qinf)	Número de documents (actes, informes, valoracions i documentació del servei) acceptats sense iteracions o amb una única iteració en la seva elaboració	Qinf = nº documents entregats amb més d'una iteració per manca de qualitat	Qinf	200 € per document amb més d'una iteració per manca de qualitat
Qualitat dels productes auditats	Número de productes auditats amb resultat de No	Qaud = nº productes auditats amb resultat de No	Qaud	1.000 € per producte auditat amb resultat de



(Qaud)	conformitat	conformitat		No conformitat
Temps de resolució de petició (Pet Tres)	Temps que transcorre entre la comunicació d'una petició i la seva resolució efectiva.	Pet Tres = Data resolució petició - data d'entrada petició	Pet Tres <= 5 dies laborables	200 € per petició que incompleixi l'ANS
Preavis per substitució (Pre Subs)	Temps que transcorre entre la comunicació oficial per escrit d'una substitució i la sortida del treballador/a.	Pre Subs = Data sortida del treballador/a - data comunicació de la substitució	Pre Subs >= 10 dies laborables	3.000 € per substitució que incompleixi l'ANS
Substitució d'un treballador/a (Subs Treb)	Temps que transcorre entre la data necessària d'arribada d'un nou treballador/a (mínim 5 dies laborables abans de la sortida del treballador/a substituït) i la seva incorporació real amb perfil validat per l'IMI al contracte.	Subs Treb = Data de sortida del treballador/a substituït - la data d'incorporació real al contracte del nou treballador/a (**)	Subs Treb >= 5 dies laborables	500 € per dia laborable que s'incompleixi l'ANS
Certificacions en cas de substitució d'un treballador/a (Cert Subs)	Compliment en cas de substitució d'un treballador/a de les certificacions obligatòries exigides al contracte (apartat 5.1.2.2 del plec) i les millores ofertes per l'adjudicatari.	Verificació en cas de substitució d'un treballador/a del compliment de les certificacions obligatòries exigides al contracte (apartat 5.1.2.2 del plec) i les millores ofertes per l'adjudicatari.	Cert Subs = Sí es compleixen totes les certificacions	1.000 € si incompleix l'ANS (s'aplicarà en cada factura mensual fins que es tinguin les certificacions necessàries)
Qualitat informació tiquets manteniment (Qitm)	Falta de qualitat de la informació en els tiquets de manteniment	Qitm = nº tiquets de l'eina de ticketing tancats amb falta de qualitat (***)	Qitm	100 € per tiquet tancat identificat a l'eina de ticketing amb falta de qualitat
Imputacions passades (Ipass)	Imputacions realitzades en mesos anteriors al tancament actual	Ipass= Import de les hores imputades en períodes anteriors al tancament actual	Ipass=0	Import de les hores imputades en períodes anteriors al tancament actual

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.



(*) Veure apartat 5.2. En el cas de la documentació per als comitès i , la data prevista és mínim 2 dies laborables abans del comitè. Es penalitzarà si es supera en un dia aquest límit, és a dir si s'entrega la presentació amb menys de 3 dies d'antelació respecte al comitè.

En el cas de les actes, s'han d'enviar abans de 2 dies laborables després del comitè. També es penalitzarà si es supera en un dia aquest límit, és a dir, si s'envia passats 3 dies de la data del comitè.

(**) En el cas que al finalitzar el mes el treballador/a no s'hagi incorporat, s'utilitzarà pel càlcul de l'ANS mensual, com a "Data d'incorporació real al contracte del treballador/a" el darrer dia laborable del mes. Aquest càlcul es continuarà realitzant cada mes, per calcular l'ANS, fins que s'incorpori el treballador/a.

(***) És responsabilitat de l'adjudicatari complimentar a l'eina de ticketing de forma detallada la informació del seu origen i causa, tractament, anàlisi i resolució. Igualment, serà responsabilitat de l'adjudicatari, mantenir actualitzat l'estat del ticket en l'eina de gestió d'incidències (actualment HPSM), en cas que aquestes no es creïn directament a l'eina de ticketing

8.1.6. Aplicació de pegats de sistema

Es requereix que s'apliquin els pegats de sistema en un temps màxim en dies (detallats a continuació), a comptar des de la data publicació de la solució/pegat a les webs oficials, segons la prioritització que té en compte:

- la criticitat de la vulnerabilitat (segons l'indicador públic CVSS)
- el nivell d'exposició (exposat o no a internet de manera oberta, sense requerir connexions VPN)
- criticitat de l'actiu
 - Estratègic: per Webs o aplicatius publicats a la ciutadania, i amb alt volum de visites o contingut sensible.
 - Estàndard: Webs o aplicatius interns o bé no publicitats, o amb nivell molt baix de visites.

		Nivell d'exposició			
		Exposat a internet		No exposat a internet	
		Criticitat de l'actiu		Criticitat de l'actiu	
		Estratègic	Estàndard	Estratègic	Estàndard
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

8.1.7. Disponibilitat de la infraestructura

Per tal d'assegurar la correcta aplicació dels ANS, s'ha establert un criteri de criticitat de les incidències, i per altra banda es té en compte la talla del web.



Funcionalitats afectades	Tipologia resultant
Afecten de forma crítica als processos de negoci i el seu incorrecte funcionament produeix un elevat impacte als usuaris	Crítiques/greus
Afecten de forma crítica als processos de negoci però el seu incorrecte funcionament no té impacte directe per als usuaris	Normals
Les afectacions sobre els processos de negoci no són crítiques i no produeixen impacte als usuaris	Consultes Altes (=Configuracions)

Plantejant la següent criticitat global (s'inclouen les aplicacions més rellevants, a tall d'exemple. A l'inici del contracte s'establirà per totes les aplicacions existents en el moment de la transició):

		Incidències					
WEB	Tipus	Consultes	Altes	Normals	Crítiques	Monitorització Activa	Disponibilitat Infraestructura
Drupal, Wordpress, Python/Django	Web CMS Estratègica	X	X	X	X	X	99,90%
	Web CMS Estandard	X	X	X			99,50%
	Web CMS Desenvolupant	X	X				99,00%
	Temps de Contacte	1,5 dies	1,5 dies	4h	2h		
	Temps de Resolució	3 dies	3 dies	1 dia	4h		
		Incidències					
Aplicacions	Aplicació	Consultes	Altes	Normals	Crítiques	Monitorització Activa	Disponibilitat Infraestructura
	Palantir	X					99,90%
	Generador Barres	X		X	X		99,90%
	Monitorització	X	X	X	X	X	99,90%
	Sysgow/Sysgox	X		X	X	X	99,90%
	Temps de Contacte	1,5 dies	1,5 dies	4h	2h		
Temps de Resolució	3 dies	3 dies	1 dia	4h			
		Incidències					
Serveis	Servei	Consultes	Altes	Normals	Crítiques	Monitorització Activa	Disponibilitat Infraestructura
	Frontals (1)	X		X	X		99,99%
	Cluster BBDD (1)	X		X	X		99,99%
	SALT (1)	X					99,99%
	BareOS (1)	X					99,99%
	Gitlab	X		X	X		99,99%
	Temps de Contacte	1,5 dies	1,5 dies	4h	2h		
Temps de Resolució	3 dies	3 dies	1 dia	4h			

En el cas d'incidències excepcionals, el Responsable del Servei corresponent de l'IMI, té la potestat de determinar que la incidència concreta queda fora d'algun dels ANS anteriors.



9. REQUERIMENTS ESPECÍFICS

En aquest apartat, es recullen els requeriments específics per a la prestació dels serveis objecte d'aquest contracte..

9.1. SER0188 Infraestructures web

Tota la gestió del contracte es fa sobre un mateix servei: SER0188 Infraestructures web, que inclou tant la gestió de la infraestructura (actualment de cloud públic a AWS), com el desenvolupament d'eines internes o de webs a ciutadà (en tecnologies PHP o Python).

Les tecnologies estan detallades a l'apartat **4.5.1 "Entorn cloud públic AWS"**.

A l'Annex 1 es troba detallada la infraestructura cloud AWS, i a l'Annex 2 es troben detallats els serveis i les seves volumetries.

9.2. Requisits generals del cloud privat de l'IMI

Adicionalment als requisits particulars, **en els casos que apliqui (a confirmar per el cap de projecte de l'ajuntament segons el cas)**, tot procés o funcionalitat haurà de contemplar els següents requisits de caràcter general:

9.2.1. Usabilitat

Usabilitat Per Aplicacions Externes (Internet).

Per a aplicacions internet cal assegurar el compliment dels requisits de prioritat 1 i 2 de la norma UNE 139803:2012 (equivalent a nivell AA en WCAG 2.0).

Les versions de navegador mínimes suportades han de ser Mozilla Firefox 68, Google Chrome 37, Safari 7.1 (IOS 8), Microsoft Internet Explorer 9 i Edge 12. L'Ajuntament proporcionarà els elements de la imatge corporativa i indicacions de com utilitzar-los per tal que se segueixi la normativa gràfica de l'Ajuntament de Barcelona.

Usabilitat Per Aplicacions Internes (Intranet)

El navegador corporatiu (amb el qual han de funcionar totes les aplicacions) serà Firefox, actualment la versió 68, i quan ja no hi hagi aplicacions amb applets Java (no javascript!) a l'Ajuntament amb futures versions.

RU1. [Obligatori] Com a criteri general, s'ha de separar el contingut de la presentació, ajustar-se a l'especificació CSS 2.1 del W3C (World Wide Web Consortium) utilitzant les Fulles d'Estil proporcionades per l'Ajuntament de Barcelona.

Per aconseguir aquest objectiu s'han de complir els requisits i consideracions definides a les guies d'estil de l'Ajuntament.



RU2. [Obligatori] La presentació s'ha de visualitzar correctament amb els navegadors Firefox vers 69 o posteriors.

RU3. [Obligatori] El temps d'aprenentatge del sistema per un usuari haurà de ser menor a 4 hores.

RU4. [Obligatori] El sistema disposarà de manuals d'usuari estructurats adequadament.

RU5. [Obligatori] El sistema ha de proporcionar missatges d'error que siguin informatius i orientats a usuari final.

RU6. [Obligatori] El sistema haurà de disposar d'un mòdul d'ajuda en línia.

RU7. [Obligatori] L'aplicació Web, si aplica, ha de posseir un disseny "Responsive" i Multi dispositiu, a fi de garantir l'adequada visualització a múltiples dispositius: DeskTop, Tables i Telèfons Intel·ligents.

RU8. [Obligatori] Si existeix el requeriment d'utilització de l'aplicació en dispositius mòbils, caldrà desenvolupar l'aplicació com a una PWA (Progressive Web Application).

9.2.2. Eficiència

L'adjudicatari haurà de garantir que tots els processos transaccionals es poden executar en un temps màxim de 3 segons. Seran una excepció aquells processos que s'hagin identificat com a pesats, segons indiqui el departament d'Arquitectura de l'IMI i s'hagi acordat en fase d'anàlisi un rang de temps d'execució superior, en aquests casos s'haurà de garantir que aquest rang de temps acordat no es veu superat.

RE1. [Obligatori] Tota funcionalitat del sistema i transacció de negoci ha de respondre a l'usuari en menys de 3 segons en el 90% de les peticions. I podem afegir la següent informació a tenir en comte:

- 0.1 segons és el límit perquè l'usuari senti que el sistema reacciona instantàniament, és a dir, que no es necessita cap retroalimentació especial, excepte per mostrar el resultat.
- 1-3 segons és el límit del flux de pensions de l'usuari per mantenir-se ininterrompuda, tot i que l'usuari observarà el retard. Normalment, no es necessita cap retroalimentació especial durant els retards de més de 0,1 però inferiors a 1,0 segons, però l'usuari perd la sensació de operar directament sobre les dades.
- 10 segons és el límit per mantenir l'atenció de l'usuari centrada en el diàleg. Per a retards més llargs, els usuaris hauran de realitzar altres tasques mentre espera que acabi l'ordinador, de manera que se'ls hauria de proporcionar informació que indiqui quan s'espera que l'ordinador es faci. La retroalimentació durant el retard és especialment important si el temps de resposta és molt variable, ja que els usuaris no saben què esperar.



RE2. [Obligatori] El sistema ha de ser capaç d'operar adequadament amb els usuaris amb sessions concurrents que es requereixen per necessitats de negoci.

RE3. [Obligatori] El sistema ha de ser tolerant a errors.

RE4. [Obligatori] El sistema ha de garantir la integritat de les transaccions.

En quant als processos batch l'adjudicatari haurà de garantir que es poden executar dins la finestra temporal, tenint en compte l'arquitectura de maquinari i de programari disponible. També cal tenir en compte que el número de processos batch a executar cada dia és molt elevat i cal permetre l'execució simultània de més d'un procés de diferent tipologia alhora.

9.2.3. Validacions de camps

Tots els processos han de fer les validacions que es defineixin per a cada camp.

- Les funcionalitats per pantalla hauran de fer les validacions i informar de les incidències a l'usuari per a la seva correcció.
- Els processos massius hauran de fer les validacions i guardar les incidències.
 - Proporcionar una funcionalitat àgil per a la consulta i correcció de les incidències que permeti correccions individuals o massives (quan una incidència es repeteixi en més d'un registre).
 - Correccions automàtiques per defecte (per corregir errors coneguts)
 - S'haurà de poder triar entre processar els registres correctes o esperar a processar a què tots els registres hagin estat corregits.

9.2.4. Logs d'execució dels processos batch

Tots els processos batch han d'extreure uns logs d'execució que permetin a l'usuari interpretar els resultats dels processos en base a unes estadístiques i permetre conèixer si hi ha hagut algun comportament incorrecte. Aquests logs han de ser entenedors per l'usuari i d'ús fàcil i particular per a cada procés.

9.2.5. Calendaris i valors per defecte

Hi haurà camps que hauran de tenir valors per defecte, aquests valors hauran de ser administrables.

També hi haurà d'haver una funcionalitat per administrar el calendari de festius i laborables que hauran de fer servir altres funcionalitats com per exemple les de notificacions per evitar el final del termini de pagament en festiu.

9.2.6. Processos massius

Degut als grans volums de registres que gestiona l'Ajuntament de Barcelona tots els processos s'han de poder executar massivament a partir d'una relació de casos d'entrada.



Això a part de l'execució un a un que òbviament també ha d'existir. Tot procés massiu ha de generar el resultat de l'execució indicant els valors necessaris per cada procés.

9.2.7. Processos en batch i on-line

Igualment i pel mateix motiu que el punt anterior tot procés s'ha de poder executar al moment (online) o en batch quan es defineixi (via planificador). Pels processos batch serà de gran rellevància analitzar la possibilitat de simultaneïtat entre els diferents processos, els objectes afectats i l'ordre d'execució que cal mantenir. Aspectes que caldrà tenir en compte:

- **Paral·lelització de cadenes:** S'analitzaran les restriccions funcionals i/o tècniques que condicionin les seqüències de la seva execució.
- **Bloquejos estàndards/a mida:** S'avaluaran els bloquejos d'objectes o elements que es produeixin per part de la solució estàndard o bé per part del programari desenvolupat a mida.
- **Rendiment del SW:** S'analitzaran les millores de rendiment del programari.
- **Eficàcia i eficiència:** S'analitzaran els aspectes per optimitzar l'eficàcia i eficiència dels processos Batch afectats.
- **Re arrancada:** en cas de cancel·lació del procés s'haurà de tenir en compte com continuar executant el procés amb el que implica per al resultat final (tractant el pendent i obtenint un resultat complet de tota l'execució).

El proveïdor presentarà un pla d'execució dels processos batch que passarà a validació de l'IMI tenint en compte tots aquests aspectes amb la suficient antelació per la seva planificació i posada en productiu.

9.2.8. Planificador batch UC4

Les operacions batch a executar de manera planificada seran gestionades des d'una eina de planificació (actualment el planificador UC4 v9) on es controlin les execucions, l'estat de l'execució, si ha acabat amb èxit o no i l'alerta al client en cas necessari.

L'usuari proporcionarà per cada nou procés batch a incloure la informació sobre què s'ha d'executar, quan i en quines condicions i la documentació associada al procés. També s'especificaran les condicions en què es podran demanar canvis urgents en processos batch planificats. L'adjudicatari serà el responsable de la confecció dels jobplans segons indicacions del departament d'Explotació de l'IMI (Of.batch) en tots els entorns necessaris i amb suficient antelació com perquè aquests siguin homologats per aquest departament. Serà imprescindible provar els diferents processos batch en entorn de pre-producció abans que s'executin en entorn productiu.

9.2.9. Retrocessió



Qualsevol operació ja sigui individual o massiva, tant batch com online, s'ha de poder retrocedir. S'entén per retrocedir retornar a l'estat anterior a l'operació, guardant traça a l'històric i fent els moviments de correcció oportuns (és a dir, mai esborrant).

9.2.10. Geocodificació d'adreces

Qualsevol adreça que es guardi al sistema haurà de ser prèviament validada contra la geocodificació estàndard de l'Ajuntament, ja sigui el procés massiu o individual, i tant batch com online. Si hi hagués dificultats o incompatibilitats tècniques, l'adjudicatari col·laborarà amb els ajusts que siguin necessaris per fer-ho possible.

La Geocodificació, en el àmbit dels sistemes de GEU fa referència a:

- Validació, normalització i obtenció d'adreces postal
- Obtenció de carrer-numero pis-porta (si aplica), districte, barri i coordenada

L'adreça sempre es recollirà i s'emmagatzemarà amb el format estàndard i normalitzat establert per l'Ajuntament de Barcelona.

En el cas de la GEU els processos de geocodificació dels elements de la via pública poden requerir la gestió de sistemes de geocodificació més complexos, complementaris als estàndards, per exemple, utilitzant polígons addicionals com poden ser els parcs o els polígons de vialitat. Serà responsabilitat de l'adjudicatari aplicar i aportar millores aquests processos de geocodificació donat el gran volum d'informació a gestionar sobre la via pública per part d'aquesta gerència.

Per la seva banda les coordenades dels diferents elements, sigui d'adreces postals, elements puntuals de la via pública (fanals, arbrat, etc.), línies o polígons, s'emmagatzemaran en projecció ETRS89 i en el format de coordenades que estableixi l'Ajuntament per cada servei (tresor, oracle locator, oracle spatial).

9.2.11. Notificació electrònica

Tot procés de notificació que s'implementi haurà de contemplar la possibilitat de notificar electrònicament a través dels serveis estàndard de l'IMI. Això implica obtenir la llista de persones que sol·licitin la subscripció a la notificació electrònica i la generació de la notificació i integració amb el mòdul comú de Notificació electrònica.

9.2.12. Generació de documents

Tots els impresos que es necessitin (cartes, llistats o informes) hauran de basar-se en el model plantilla:

- amb contingut fix administrable per l'usuari final (els que a tal efecte es determinin).
- contingut variable format per dades provinents de les aplicacions.
- bilingües català i castellà en el mateix document (en monolingües si es disposa de la preferència del contribuent).



Hauran de complir els següents requisits:

- S'hauran de poder generar individualment o de forma massiva i en mode online o en batch.
- Seguint criteris de minimització i reutilització de plantilles.
- Generables en formats RTF, PDF i JPG.
- Exportables a Word, Excel, fitxer pla.
- Hauran de servir per ser utilitzats per tots els canals de tramitació: presencial, telefònic, internet, mòbil, quiosc.

S'haurà de tenir en compte que els documents es carregaran al gestor documental i des dels serveis s'hi haurà de poder accedir.

Els requisits tècnics i la plataforma a utilitzar es descriuen a l'apartat corresponent.

El proveïdor serà el responsable de la gestió de la generació i validació dels documents i plantilles afectats per part de l'usuari amb el temps suficient i accions de seguiment per disposar-ne abans de cada posada en marxa. Si és necessari definirà el procediment d'aprovació dels documents.

9.2.13. Publicació d'edictes

La publicació al butlletí corresponent amb l'edecte corresponent i opcionalment al tauler d'edictes de l'Ajuntament de Barcelona.

9.2.14. Assignació de rols

1. Autenticació d'usuaris

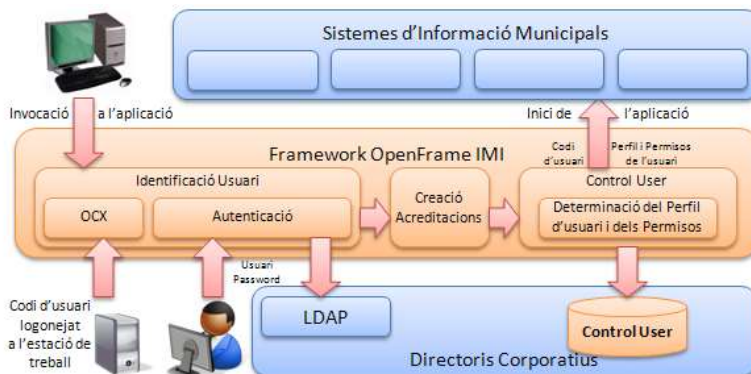
Per a les aplicacions que s'executen internament des de la pròpia xarxa de l'Ajuntament, es disposa de diferents serveis per a l'autenticació dels usuaris, que no difereixen en la seva funcionalitat si no tan sols en la necessitat d'adaptació per a les diferents plataformes.

Per a aplicacions J2EE les funcions estan integrades a la capa de seguretat de l'OpenFrame IMI. Per a aplicacions .NET les funcions estan desenvolupades al NET Framework de l'IMI

Els aplicatius basats en navegador, J2EE i .NET, a més incorporen en els respectius Frameworks una funció addicional que, basada en un component SSO que s'executa a l'estació de treball, identifica el codi d'usuari que ja ha estat prèviament autenticat a aquesta estació de treball i utilitza aquest codi per a la identificació de l'usuari estalviant que aquest hagi de teclejar el seu identificador i paraula clau, tret que l'identificador reconegut a l'estació de treball no correspongui a un codi personal d'usuari, cosa que provocarà que el sistema demandi aquestes dades a l'usuari.

Un cop efectuada l'autenticació (per codi d'estació de treball o per usuari i clau d'accés informats) es procedeix a determinar el perfil i els permisos de que es disposarà a l'aplicació

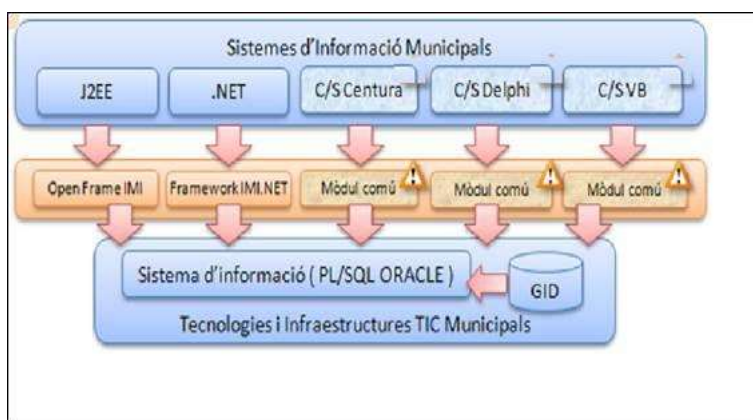
durant la sessió present. Per a aquesta funció s'utilitza el sistema general anomenat "Control User", i que es descriu a l'apartat Gestió de perfils i permisos d'usuaris "CtrlUsr".



Finalment es dona control a l'aplicació informant del codi d'usuari que hi accedeix i del perfil i permisos que ostentarà.

2. Gestió d'Usuaris i Permisos

La CtrlUsr es el sistema d'informació que permet gestionar l'autenticació i l'autorització dels usuaris a les aplicacions, mitjançant un catàleg d'aplicacions, una llista de funcions agrupades en perfils i aquets perfils assignats a usuaris. Aquest sistema d'informació, és utilitzat en totes les plataformes de desenvolupament de l'IMI (a excepció de Host i SAP).



9.2.15. Llistats, informes i explotació de la informació

S'hauran de configurar en les eines que l'IMI disposi o en el seu defecte desenvolupar tots els llistats necessaris per garantir l'operativa diària de la GEU de l'Ajuntament de Barcelona. A l'inici del contracte, l'IMI proporcionarà la documentació associada a cadascuna de les eines esmentades.

Aquests llistats s'hauran de poder:

- Imprimir, amb les capçaleres i peus corresponents.



- Exportar a formats PDF, RTF, CSV, fitxer pla, MS Word i MS Excel.
- Basats en model plantilla: amb contingut fix administrable per l'usuari final (els que a tal efecte es determinin en la fase funcional del contracte) i contingut variable format per dades provinents de les aplicacions.

Es requerirà disposar de dades de detall i de dades agregades per a totes els entitats.

S'haurà de poder realitzar extraccions (per exportar a altres sistemes) i informes combinant informació de les diferents entitats.

9.2.16. Proves de Càrrega

Abans de l'entrada en producció d'una funcionalitat, s'hauran de definir i executar les proves de rendiment i estrès que garanteixin el correcte funcionament. Per dur a terme aquestes proves, l'adjudicatari haurà de preveure el suport a aquestes proves, així com el desenvolupament dels jocs de dades necessaris.

L'objectiu és garantir els temps d'execució dels processos transaccionals definits en el punt anterior.

Adicionalment, s'hauran de fer proves d'execució i rendiment dels processos batch pesats per a la seva optimització i per assegurar que es poden executar dins la finestra que es defineixi en la presa de requisits, així com assegurar que es poden executar simultàniament amb altres processos pesats ja existents.

9.2.17. Proves de Regressió

Abans de l'entrada en producció d'una funcionalitat important o d'un canvi tecnològic rellevant amb afectació transversal, s'haurà de revisar i acordar amb l'IMI el fet de definir i executar les proves de regressió que provin les funcionalitats del sistema i que garanteixin el correcte funcionament. Per dur a terme aquestes proves, l'adjudicatari haurà de preveure el suport a aquestes proves, així com el desenvolupament dels jocs de dades necessaris. Les proves de regressió a efectuar poden ser de nivell bàsic (funcionalitats clau) o complet.

9.2.18. Monitorització del servei

L'adjudicatari haurà de proporcionar uns casos d'ús que permetin contestar si l'aplicació està operativa. Aquests casos d'ús s'han de poder executar, tant puntualment de manera manual, com estar programats en un robot que els realitza amb una certa periodicitat (en aquest moment cada 10 minuts). Òbviament s'ha de preveure que aquests casos d'ús siguin significatius, el mínim intrusius possible i que no afectin als processos de negoci. L'IMI col·laborarà amb l'usuari i l'adjudicatari en la definició del millor cas d'ús possible.

9.3. Requisits d'arquitectura del cloud privat de l'IMI

Adicionalment als requisits particulars, en els casos que apliqui (a confirmar per el cap de projecte de l'ajuntament segons el cas), tot procés o funcionalitat haurà de contemplar els següents requisits d'arquitectura:



RA1. [Obligatori] Llenguatges de programació i Frameworks

Els llenguatges “base” per programar les aplicacions a mida a l'Ajuntament de Barcelona són JavaEE i Python. Per les webs del cloud públic s'utilitza PHP aplicat a Drupal i Wordpress.

Quan el llenguatge “base” sigui JavaEE l'IMI disposa d'un framework propi de anomenat OpenFrameIMI i que, actualment, es troba en la versió 4. Aquest framework és d'**obligatori utilització** per al desenvolupament d'aplicacions Java. Cal destacar que el framework openFrameIMI fixa l'arquitectura i els serveis per les capes de Negoci, integració i persistència.

Quan el llenguatge “base” sigui Python, el framework ha de ser Django/Python.

El frameworks de l'IMI **No fixen la capa de presentació**, però aposten per front-ends (SPAs Single Page Applications) que han d'estar implementats en Angular (en la seva versió estable).

RA2. [Obligatori] Preparada per a ser Desplegada en Cloud

El desenvolupament del sistema caldrà estar orientat a serveis. Tot el negoci de l'aplicació ha d'exposar-se mitjançant una o més API(s) de serveis.

Aïllar els serveis que l'aplicació necessita per a funcionar i implementar-ho com a una API independent, permetrà a aquest tenir la capacitat d'adaptar-se i escalar segons la càrrega o peticions que rebi, sense afectar a la resta de l'aplicació. A la mateixa vegada aquest disseny permet monitoritzar i gestionar amb més precisió els diferents components de software.

La construcció de l'aplicació haurà de seguir els [12 Factors App](#):

I. Codi base (codebase)

Un codi base sobre el qual fer el control de versions i múltiples desplegaments

II. dependències

Declarar i aïllar explícitament les dependències

III. configuracions

Guardar la configuració en l'entorn

IV. backing services

Tractar als "backing services" com a recursos connectables

V. Construir, desplegar, executar

Separar completament l'etapa de construcció de l'etapa d'execució



VI. processos

Executar l'aplicació com un o més processos sense estat

VII. Assignació de ports

Publicar serveis mitjançant assignació de ports

VIII. concurrència

Escalar mitjançant el model de processos

IX. Desechabilidad

Fer el sistema més robust intentant aconseguir inicis ràpids i acabaments segures

X. Paritat en desenvolupament i producció

Mantenir desenvolupament, preproducció i producció tan semblants com sigui possible

XI. historials

Tractar els historials com una transmissió d'esdeveniments

XII. Administració de processos

Executar les tasques de gestió / administració com a processos que només s'executen un cop

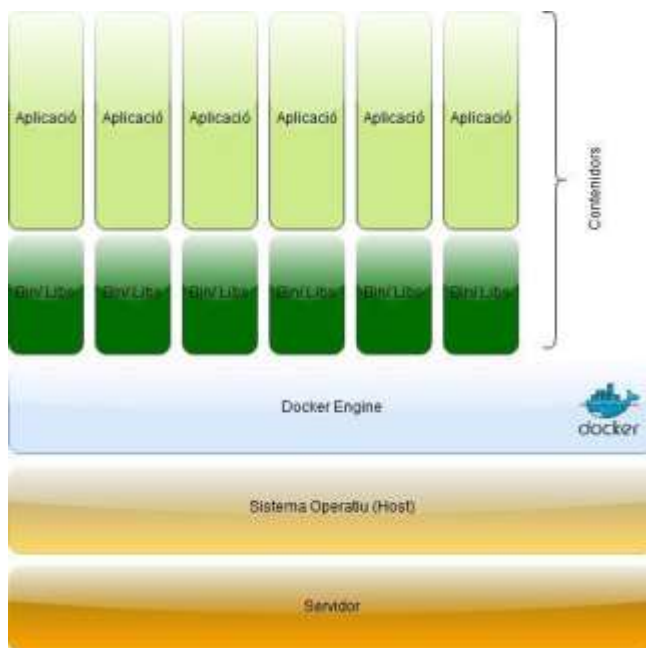
RA3. [Obligatori] Preparada per a ser Desplegada en contenidors dockers

Caldrà orientar les aplicacions al funcionament en contenidors Dockers, replicant d'aquesta manera als contenidors la mateixa infraestructura productiva. Per això es partirà d'imatges preparades per l'IMI que s'hauran de fer servir de base per a la construcció de les imatges definitives que caldrà desplegar.



Aconseguirem amb això els següents objectius:

- Igualar els entorns el màxim possible.
- Simplificar la Instal·lació: Al fer servir imatges mestres preparades a tal efecte.
- Independitzar-se de la plataforma: Les imatges amb els contenidors es poden canviar d'un sistema a un altre facilitant no només els canvis a nivell productiu sinó les proves a entorns locals o de desenvolupament.
- Aïllar les aplicacions: Cada aplicació pot o no compartir contenidors de forma que es poden aïllar segons les necessitats existents.
- Automatitzar l'administració.



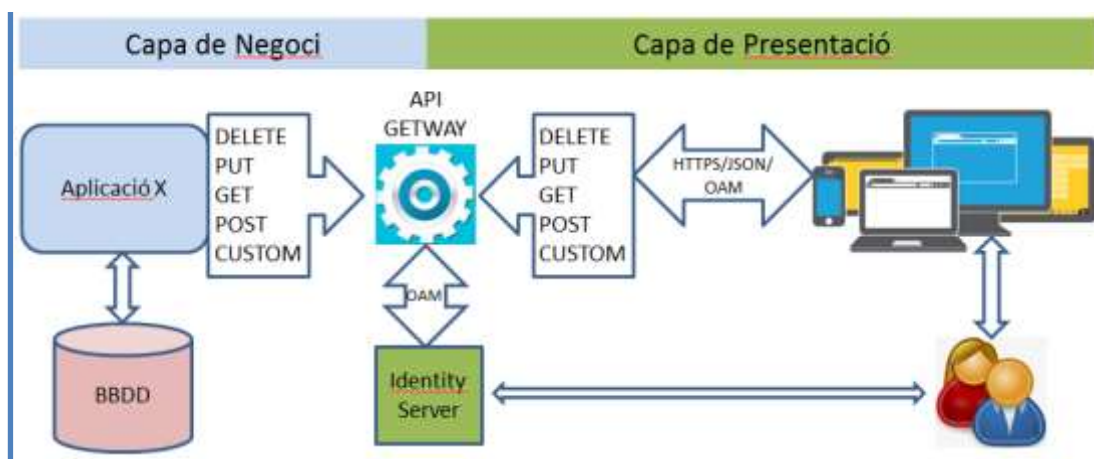
RA4. [Obligatori] Requisits de modularitat i escalabilitat

Per eficiència i sostenibilitat el sistema a construir haurà de ser modular i escalable: ha de tenir un enfocament prou transversal com per minimitzar l'impacte de la incorporació de noves funcionalitats.

RA6. [Obligatori] Arquitectura del sistema

Les diferents aplicacions que es desenvolupin per donar compliment als requeriments funcionals tindran un disseny tècnic modular i escalable.

Hi ha tres Components Diferents Implicats en el disseny de l'Arquitectura: L'Aplicació(Negoci), l'API Gateway i el client(Presentació). La imatge de sota Il·lustra com interactuen AQUESTS 3 components.



Capa de Negoci

Cada aplicació disposarà d'una capa de negoci, desenvolupada amb openFrameIMI (en el cas de J2EE), amb les funcionalitats de negoci i l'accés a la base de dades. Aquesta capa només accepta dades i només serveix dades.

- Desenvolupada amb la última versió disponible de openFrameIMI en cas de Java, o una altre de les tecnologies acceptades per l'IMI
- Arquitectura RESTful sense sessió al costat del servidor
- L'aplicació no proporciona interfície d'usuari. El que proporciona és un conjunt d'API(s) amb:
 - Consultes de les entitats del model de dades.
 - Manteniment de les entitats del model de dades.
 - Les funcionalitats de negoci.
- L'aplicació farà servir les API(s) dels diferents serveis comuns IMI o d'altres aplicacions per tal de interactuar amb aquests sistemes.
- Les API(s) es publiquen a l'API Manager sense excepció i no poden ser consumides fora d'ell.

Capa de Presentació

Cada aplicació disposarà d'una capa de presentació per generar la GUI dels usuaris.

- La capa de presentació és la responsable de generar les pantalles a l'usuari i d'atendre les seves peticions. **No ve fixada pel framework de l'IMI.**
- **Pot** estar basada en el framework estàndard per a aplicacions SPA de l'IMI: Arquitectura Angular5 + Bootstrap com framework de presentació. És responsable de generar les pantalles a l'usuari i d'atendre les seves peticions.
- No té a dins llibreries ni per resoldre funcionalitats de negoci ni per accedir directament a base de dades ni per accedir als elements tercers a integrar.



- Totes aquestes funcionalitats les delega en l'aplicació de la capa negoci descrita abans cridant a les seves API(s) RESTful.
- Les API(s) es consumeixen mitjançant l'API Manager, **mai** directament.
- L'aplicació s'integrarà amb els serveis oferts per la plataforma de seguretat OAM per cobrir tant l'autenticació com l'autorització.
- **Si es fa servir** la presentació SPA inclosa en el framework:
 - Farà servir el conjunt de controls visuals per aplicacions de la Intranet de l'Ajuntament, inclosos al framework, adaptats a la guia d'estils per aplicacions de la Intranet de l'Ajuntament.
 - Proporciona un entorn de desenvolupament Local:
 - Un instal·lador per a les eines següents:
 - nvm (si es prepara per desenvolupar en linux) o nvm-windows o nodist (si es prepara per desenvolupar en MS Windows)
 - Visual Studio Code.
 - Preconfiguració per forçar la versió de Node.js decidida per l'IMI.

Serveis (Negoci) – Noves aplicacions

- L'instal·lable haurà de seguir una arquitectura de "*monòlit modular*" no pas de *microserveis*.
- Es farà una divisió en instal·lables de l'aplicació basada en funcionalitats. Cadascun d'aquests instal·lables donarà compliment a uns requisits funcionals concrets de l'aplicació.
- Els serveis s'implementaran RESTful sense sessió al costat del servidor proporcionant:
 - Consultes de les entitats del model de dades.
 - Manteniment de les entitats del model de dades.
 - Funcionalitats de negoci.
- Per consumir serveis comuns d'altres aplicacions s'utilitzarà els serveis publicats a l'API Manager. Aquests serveis es diferencien en dos tipus:
 - Serveis públics, només cal tenir un clientId per consumir-los.
 - Serveis privats o autenticats, cal autenticació amb un usuari (nominal o de servei) per tal de poder consumir el servei.
 - Això comporta fer una autenticació amb l'usuari per obtenir un token i enviar aquest token en totes les crides al servei junt amb el clientId.
- Les API(s) es publiquen a l'API Manager sense excepció i no poden ser consumides fora d'ell.

Publicació a l'API Manager

- Cal especificar el/s servei/s en un fitxer swagger (format yaml) per tal de publicar-lo a l'API Manager



- Aquesta publicació té entitat pròpia i requereix tenir-la en compte al projecte.

Client (Presentació)

- Cada aplicació disposarà d'una capa de presentació per generar la GUI dels usuaris.
- La capa de presentació és la responsable de generar les pantalles a l'usuari i d'atendre les seves peticions. No ve fixada pel framework de l'IMI.
- Pot estar basada en el framework estàndard per a aplicacions SPA de l'IMI: Arquitectura Angular5 + Bootstrap com framework de presentació. És responsable de generar les pantalles a l'usuari i d'atendre les seves peticions.
- No té a dins llibreries ni per resoldre funcionalitats de negoci ni per accedir directament a base de dades ni per accedir als elements tercers a integrar.
- Totes aquestes funcionalitats les delega en l'aplicació de la capa negoci descrita abans cridant a les seves API(s) RESTful.
- Les API(s) es consumeixen mitjançant l'API Manager, mai directament.
- L'aplicació s'integrarà amb els serveis oferts per la plataforma de seguretat OAM per cobrir tant l'autenticació com l'autorització.
- Si es fa servir la presentació SPA inclosa en el framework:
 - Farà servir el conjunt de controls visuals per aplicacions de la Intranet de l'Ajuntament, inclosos al framework, adaptats a la guia d'estils per aplicacions de la Intranet de l'Ajuntament.
 - Proporciona un entorn de desenvolupament Local:
 - Un instal·lador per a les eines següents.
 - nvm (si es prepara per desenvolupar en linux) o nvm-windows o nodist (si es prepara per desenvolupar en MS Windows).
 - Visual Studio Code.
 - Preconfiguració per forçar la versió de Node.js decidida per l'IMI.

RA7. [Obligatori] Estructura multi-idioma

La solució ha de ser multi-idioma. La totalitat dels camps/missatges visibles per l'usuari han de poder traduir-se a taules, de manera que la incorporació d'un o un altre idioma no suposi haver de revisar i traduir codi font. El multi-idioma aplica als *tags* associats a llistats, pantalles i documents així com als missatges que generi el sistema en les diferents pantalles, incloent pantalles d'ajuda. El multi-idioma no aplica al contingut de la base de dades (informació associada al *data entry*).

L'IMI requereix que l'aplicació vingui configurada inicialment en català, si bé es demanarà la visualització d'un parell de pantalles, documents, llistats i missatges en castellà per comprovar el correcte funcionament de la característica multi-idioma del sistema construït.

La documentació que es generi en el transcurs del contracte només s'haurà d'entregar en català.



RA8. [Obligatori] Traçabilitat

Adicionalment, el sistema haurà de garantir la traçabilitat de les accions dels usuaris sobre el mateix.

RA9. [Obligatori] Components de software lliure

L'IMI advoca per reduir el nombre de components de software amb llicència, i recomana per tant l'ús de components de codi obert.

RA10. [Obligatori] Entorns per aplicacions

L'IMI disposa de 4 entorns per a l'execució d'aplicacions:

- **Entorn local:** el desenvolupament es fa en el PC del desenvolupador. Aquest entorn permet fer totes les proves i integracions necessàries del producte.
- **Entorn d'integració:** en aquest entorn s'instal·len en primera instància les aplicacions. Permet identificar els errors d'integració amb els components de l'arquitectura de l'IMI.
- **Entorn de pre-producció:** una vegada depurats els errors d'integració, les aplicacions s'instal·len en aquest entorn. És idèntic a l'entorn de producció i permet comprovar que les aplicacions funcionaran correctament quan s'instal·lin en producció.
- **Entorn de producció:** aquest és l'entorn definitiu en què treballa l'usuari i on s'han de deixar instal·lades les aplicacions.

Totes les aplicacions lliurades a l'IMI s'han d'instal·lar, posar en funcionament i provar en aquests quatre entorns.

RA11. [Obligatori] Plataformes de desenvolupament

La plataforma d'orquestració de contenidors a l'IMI es base en **kubernetes**. Aquesta plataforma permet el desplegament, a priori, de qualsevol llenguatge de programació i/o producte que es pugui dockeritzar. No obstant, l'IMI limita les diferents tecnologies en les que es poden implementar les seves aplicacions.

Actualment l'IMI permet les següents tecnologies:

- Capa de serveis i/o de negoci
 - Java:
 - Name: apache-tomcat-8.5.34-fwk4
 - Basada en java 8v192 i Tomcat 8.5.34
 - Plataforma Python
 - versió estable
- Capa de presentació
 - Framework SPA IMI:
 - Name: nginx-alpine-1.15.5-fwkspa
 - Basada en Angular 5



- Capa d'emmagatzemament de dades
 - Oracle 11g sobre SUSE (en curs migració a Oracle 12)
 - Servidor corporatiu
 - no en contenidors
 - La BD està fora de la plataforma kubernetes
 - És una instància Corporativa, 1 únic servidor de BD per n projectes
 - L'IMI gestiona aquesta infraestructura

A més d'aquestes tecnologies, i/o llenguatges de programació, l'IMI port permetre la utilització d'altres productes com BD Redis, sistemes ELK, mongoDB destinades a accelerar, cobrir o millorar alguna funcionalitat concreta del producte resultant. No obstant, caldrà justificar clarament el perquè de la seva utilització i aquesta haurà de ser aprovada pel departament de producció, el departament de seguretat i el departament d'arquitectura de l'IMI.

9.4. Requisits de seguretat

Adicionalment als requisits particulars, en els casos que apliqui (a confirmar per el cap de projecte de l'ajuntament segons el cas), tot procés o funcionalitat haurà de contemplar els següents requisits de seguretat:

Els productes finals desenvolupats hauran de complir amb els estàndards de seguretat establerts per:

- La legislació vigent que sigui d'aplicació.
- El conjunt de bones pràctiques en matèria de seguretat TIC establert en la norma ISO- 27002:2013 i en especial la seva adaptació a l'IMI (Cos Normatiu de Criteris de Seguretat i Protecció de Dades de l'Ajuntament de Barcelona).
- El conjunt de bones pràctiques de desenvolupament de projectes Python/Django i web.
- Les instruccions i convencions establertes pel Departament de Govern de Seguretat.
- En especial aquelles establertes per l'Oficina de Seguretat TIC.
- Les instruccions i convencions establertes per l'Oficina d'Arquitectura de la Direcció de Desenvolupament de Sistemes d'informació de l'IMI.
- Aquells establerts o definits en la fase de presa de requeriments del contracte.

9.4.1. Seguretat de l'aplicació

RS2. [Obligatori] Autenticació: El sistema ha de comprovar que l'usuari que tracta d'accedir al sistema és qui diu ser. De forma general, l'autenticació dels usuaris es pot fer mitjançant els següents mecanismes:

- Usuari i contrasenya validada contra un servidor de credencials corporatiu.

Aquest requeriment es realitzarà mitjançant la utilització del sistema d'Autenticació i Autorització corporatiu.



RS3. [Obligatori] Autorització: El sistema ha d'implementar mecanismes per a restringir a usuaris no identificats i autoritzats l'accés a la informació.

Aquest requeriment es realitzarà mitjançant la utilització del sistema d'Autenticació i Autorització corporatiu.

RS4. [Obligatori] Es farà coincidir els usuaris d'aquest sistema amb els usuaris de la xarxa corporativa i evitant la reinserció de credencials (SSO).

Aquest requeriment es realitzarà mitjançant la utilització del sistema d'Autenticació i Autorització corporatiu.

RS5. [Obligatori] Xifrat de dades: La comunicació de l'usuari amb el sistema es realitzarà únicament mitjançant canals segurs (https). Els algorismes criptogràfics emprats seran els acreditats pel Centre Criptològic Nacional per al seu ús en l'Esquema Nacional de Seguretat.

RS6. [Obligatori] Gestió d'usuaris i sessions: Els mecanismes de control de sessions d'usuaris autenticats contemplaran:

- a. Tancament de sessió per part de l'usuari.
- b. Expiració automàtica de sessió.

RS7. [Obligatori] Gestió d'errors i excepcions: Es realitzarà un tractament sistematitzat i centralitzat d'errors i excepcions, eliminat la informació interna del sistema o sensible dels missatges mostrats a l'usuari.

RS9. [Obligatori] El nou sistema s'ha de desenvolupar seguint patrons i recomanacions de programació que incrementin la seguretat de les dades.

RS10. [Obligatori] Qualsevol intercanvi de dades entre serveis o aplicacions es realitzarà mitjançant API(s) de serveis fen servir el protocol encriptat HTTPS.

RS11. [Opcional] Les dades que formin part d'un fitxer de nivell ALT segons la LOPDGDD seran encriptades. No es guardaran de forma oberta a la BD i només es descriptaran per ser llegides un cop comprovat que l'usuari té el perfil necessari per veure-les.

- L'IMI indicarà quin algoritme s'ha de fer servir en cada cas.

9.4.2. Control d'accés

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 solució IDP utilitzada per l'IMI és el Reg Hat Single Sign On (RH-SSO)

La integració amb RH-SSO 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'aplicatiu) hauran d'autenticar-se mitjançant la solució corporativa (Mòdul Comú d'Autenticació).

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

9.4.3. Gestió de les Autoritzacions

L'IMI disposa d'un repositori centralitzat d'autoritzacions dels usuaris corporatius, basat en un directori actiu, que és d'on l'IDP corporatiu recull les autoritzacions. 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 (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.

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.

9.4.4. Registre d'activitats del sistema. Auditabilitat i traçabilitat

El producte final ha de garantir la imputabilitat inequívoca de qualsevol operació o tractament de dades que es faci dins el sistema. Qualsevol operació o tractament s'ha de poder imputar a un codi d'usuari, a més s'ha de poder identificar físicament la màquina des de la qual s'ha fet, la data i l'hora. És a dir, el registre de logs ha de garantir que es puguin respondre les preguntes bàsiques de qualsevol anàlisi forense: qui?, què?, quan?, cóm?, des d'on?.

Els processos sistema (batch, webservices, msgbrokers) han de permetre també un nivell d'auditoria i traçabilitat suficient per poder imputar a un procés o sistema concret una determinada operació.

Disposar d'un registre de logs que emmagatzemi totes les operacions realitzades pels usuaris que puguin afectar a informació sensible, i permeti a una persona amb l'autorització adequada accedir fàcilment a l'historial d'operacions realitzades per un usuari, així com a l'historial d'operacions realitza sobre un objecte.

9.4.5. 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 i LOPDGDD marcaran la informació que cal recollir i el temps de retenció dels logs.

- L'objecte d'aquest apartat és garantir les evidències necessàries per tal que es tractin els següents aspectes:
- Amb quina eina es recolliran les traces
- Requeriments de criticitat, legals i de negoci
- Repositori de traces, on s'indiqui clarament el lloc on es guarden les traces i el nivell d'accés i seguretat d'aquestes
- Inventari detallat de les traces que es guarden
- Pla i política d'arxiu de logs
- Mostres de les traces inventariades resultants



- L'adjudicatari s'ha de comprometre també a adaptar el Manual d'Explotació d'aquestes traces.

Amb tal propòsit, 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.

9.4.6. Emmascarament de dades de caràcter personal

Aprofundint en el concepte "privacy by design" en alguns registres productius especialment sensibles les dades de caràcter personal s'hauran de mostrar emmascarades, excepte pels perfils expressament autoritzats.

Ús de dades reals en entorns no productius

D'acord amb les bones pràctiques internacionalment reconegudes i amb la legislació vigent l'adjudicatari s'abstindrà d'utilitzar dades reals per fer proves.

Per tant, l'adjudicatari haurà de realitzar en el contracte totes les tasques relatives a la generació de jocs de proves (unitàries, d'integració, de regressió, de rendiment).

Excepcionalment amb autorització expressa del Responsable del Tractament es podran utilitzar dades reals per generar automàticament jocs de proves sempre i quan les dades siguin dissociades prèviament. D'acord amb l'AEPD aquesta dissociació haurà de ser irreversible. El cost i les eines de dissociació correran a càrrec de l'adjudicatari i s'incorporaran al contracte com una funcionalitat més que a la finalització del mateix quedarà a disposició de l'equip tècnic de l'IMI.

9.4.7. Canvi organitzatiu

Pel que fa als aspectes relacionats amb la seguretat:

- En tot cas, el model organitzatiu haurà de respectar el principi de segregació de funcions.
- El personal de desenvolupament del contracte no podrà fer servir rols tècnics per al desenvolupament del mateix.

La resta d'aspectes relacionats amb el canvi organitzatiu seguiran les instruccions i models establerts per la Direcció de l'IMI d'acord amb la seva potestat d'autoorganització.



9.5. Estàndards de desenvolupament

Adicionalment als requisits particulars, en els casos que apliqui (a confirmar per el cap de projecte de l'ajuntament segons el cas), tot desenvolupament haurà de contemplar els següents requisits:

9.5.1. Per a tecnologia Python

Es troba detallat a l'**Annex 7**, normativa Python.

9.5.2. Per a tecnologia Drupal (PHP)

Es troba detallat a l'**Annex 8**, Drupal.

9.6. Metodologia de desenvolupament

Adicionalment als requisits particulars, **en els casos que apliqui (a confirmar per el cap de projecte de l'ajuntament segons el cas)**, tot procés o funcionalitat haurà de contemplar els següents requisits en quant a la metodologia de desenvolupament:

9.6.1. Qualitat de codi

RQ1. Tot codi font que es vulgui desplegar als servidors de l'IMI requerirà el compliment dels estàndards de qualitat indicats pel mateix IMI. Aquests estàndards es concreten en l'aplicació de diferents Quality Gates.

Quality Gates actuals per Java:

- Conditions on New Code
 - **Coverage**, ha de ser superior al 30.0%
 - **Bugs**, no es permet cap bug
 - **Vulnerabilities**, no es permet cap vulnerability
- Conditions on Overall Code
 - **Blocker Issues**, no es permet **cap**.
 - **Coverage**, ha de ser, com a mínim, del **60.0%** de tot el codi del projecte
 - **Critical Issues**, no es permet **cap**.
 - **Unit Test Failures**, 0. Tots els test case han funcionar.
- El conjunt de regles de qualitat de codi de l'eina SonarQube (es revisen/actualitzen anualment).

RQ2. En cap cas les conseqüències del no compliment d'aquests estàndards podrà justificar l'endarreriment de les fites d'entrega del projecte, en cas de recepció del mateix pel servei, o l'endarreriment de noves versions del codi de serveis de manteniment, en aquest cas directament imputable a l'adjudicatari del servei.



RQ3. En cas d'aplicacions antigues, no desenvolupades des del seu inici amb els actuals llistats de qualitat, es marquen llistats de qualitat diferents.

RQ4. En qualsevol cas el proveïdor es compromet a no empitjorar el nivell de qualitat actual de l'aplicació. Això implica que el nou codi desenvolupat no empitjorarà els següents indicadors:

- Número de Bugs
- Número de Vulnerabilities
- Security Hotspots
- Security Rating
- Technical Debt Ratio

RQ5. Pel que fa a les proves unitàries. L'IMI podrà exigir que el **nou codi** compleixi amb la regla del 60% de Cobertura. No obstant això, el proveïdor podrà demanar la relaxació d'aquest llistat justificant la seva complexitat envers l'estat del desenvolupament.

- Aquesta justificació haurà de ser aprovada per la direcció de projecte, arquitectura i seguretat.
- En cap cas aquest nou llistat serà inferior al 30% de Cobertura de codi.

9.6.2. Metodologia de treball a aplicar (Dockers)

RM1. [Obligatori] L'empresa adjudicatària haurà de gestionar 4 entorns per a l'execució d'aplicacions: desenvolupament, integració, pre-producció i producció.

Entorn local: el desenvolupament es fa en el PC del desenvolupador. Aquest entorn permet fer totes les proves i integracions necessàries del producte.

Entorn d'integració: en aquest entorn s'instal·len en primera instància les aplicacions. Permet identificar els errors d'integració amb els components de l'arquitectura de l'IMI.

Entorn de pre-producció: una vegada depurats els errors d'integració, les aplicacions s'instal·len en aquest entorn. És idèntic a l'entorn de producció i permet comprovar que les aplicacions funcionen correctament quan s'instal·lin en producció.

Entorn de producció: aquest és l'entorn definitiu en què treballa les persones usuàries i on s'han de deixar instal·lades les aplicacions desenvolupades (mòduls i funcionalitats). Totes les aplicacions lliurades a l'Ajuntament de Barcelona s'han d'instal·lar, posar en funcionament i provar en aquests entorns.

RM2. [Opcional] L'aplicació ha de ser configurada perquè pugui integrar-se amb *Sentry* per a la monitorització d'errors a nivell d'aplicació.

RM3. [Opcional per a productes] És necessari que l'aplicació s'entregui de manera que sigui possible un desplegament basat en l'automatització per mitjà de *Docker* en màquines de tipus *Ubuntu/Debian*, ja sigui en servidors físics, virtuals.



RM4. [Obligatori] Les peticions, tasques, *issues* o tickets seran tractats a través del propi sistema de tickets de L'IMI.

RM5. [Obligatori] Per gestionar el codi es farà servir el gestor de codi corporatiu de l'Ajuntament, actualment GIT.

RM6. [Opcional] Els canvis en el codi hauran de pujar-se a través de *Pull Requests*, on un mínim d'una persones de l'equip del servei de l'empresa adjudicatària hauran de revisar el codi i aprovar els canvis.

RM7. [Obligatori] És responsabilitat de l'empresa adjudicatària garantir que es puguin disposar en el propi repositori de:

El codi de l'aplicació.

La llista de dependències amb altres llibreries i aplicacions lliures.

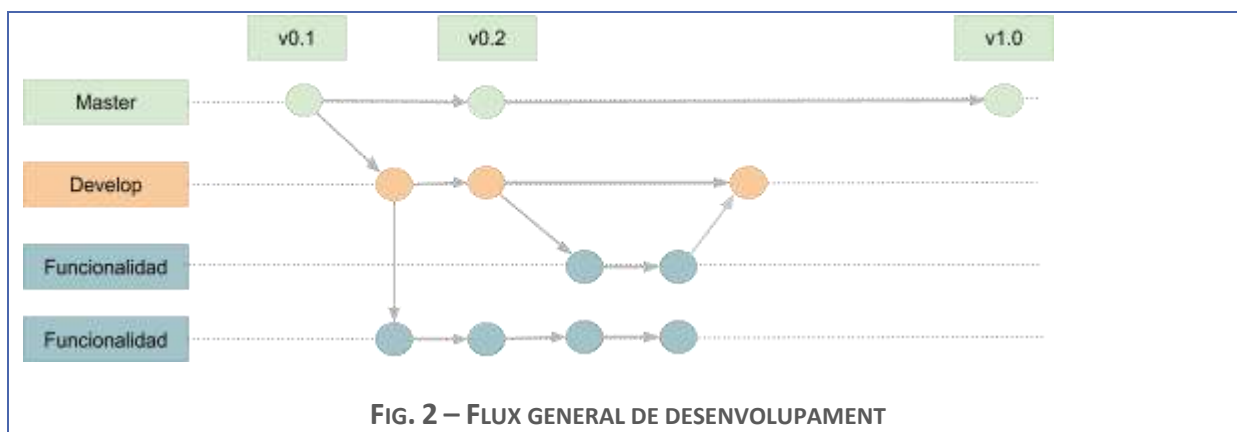
Els fitxers de generació de contenidors Docker.

RM8. [Obligatori] Com a mínim es faran servir dues branques estables:

- develop -> Contindrà el codi provat i finalitzat per desplegar a l'entorn d'integració.
- master -> Contindrà el codi provat i finalitzat per desplegar a pre-producció. Un cop validat a pre-producció ja no hi haurà més construccions. Aquesta construcció validada serà la que s'instal·larà a producció.

RM9. [Obligatori] Cada nova implementació es farà en una nova branca i s'integrarà a la branca oficial quan es consideri provat i estable.

- Esquema de funcionament:



S'aconsella l'ús de desenvolupament dirigit per tests (*test driven development*) que possibiliti la instal·lació d'un sistema d'integració contínua.

Es tracta d'una metodologia de desenvolupament de software, basada principalment en garantir la qualitat del codi, i la qual s'empra en un breu cicle que es repeteix durant tot el desenvolupament. Aquest cicle és:



1. Es prenen els requisits a desenvolupar.
2. Els requisits es converteixen en tests (abans de començar a codificar).
3. Es passa la bateria de tests ja creats i es comprova que els nous tests efectivament donen error.
4. Es desenvolupen els nous requeriments per a satisfer aquests nous tests.
5. Es passa novament la bateria de tests, i es comprova que tots queden satisfets.
6. Es re-factoritza el codi per adaptar les noves funcionalitats, cohesionant-les amb la bateria de test anterior.
7. Es torna al punt 1 si encara no s'ha acabat el producte.

Els beneficis de seguir aquesta metodologia són els següents:

La bateria de tests es manté sempre actualitzada.

El projecte esdevé robust i auto documentat.

El producte final és més fidel als requisits presos.

Detecció ràpida de desviacions en el desenvolupament.

Millora de la qualitat del producte final.

Minimització del temps dedicat a la depuració d'errors.

Minimització del temps dedicat a la fase de manteniment.

Garantia de mínim impacte en la implementació de noves funcionalitats.

Els tests han de complir una sèrie de requisits:

Han de ser auto descriptius sobre la funcionalitat que estan provant.

Han de servir com a documentació del codi.

Han de ser el més unitaris possible.

No han de dependre d'altres tests.

Han de partir d'un escenari concret i deixar els recursos alliberats tal com els van trobar a l'iniciar l'escenari.

La cobertura dels tests ha de ser el més completa possible: les funcionalitats s'han de provar en tots els casos plausibles d'esdevenir.

El tipus de tests que es desenvoluparan seran els següents:

- Tests unitaris: sobre cada classe / funcionalitat a desenvolupar.
- Tests d'integració: sobre les integracions dels diferents components entre les seves interfícies. Si els components són externs (APIs, *webservices*, etc.), es simularà aquest i la seva interacció mitjançant *mockups*.
- Tests d'interfície d'usuari: aquests ens serviran per garantir que la interfície d'usuari és robusta i completa segons les especificacions.
- Tests de rendiment: amb aquests tests garantirem que el sistema és escalable sobre els recursos proporcionats, amb un rendiment acceptable, proposat en el projecte.



- **Tests de regressió:** verifica que els canvis aplicats al producte no tenen cap impacte negatiu en les característiques que anteriorment funcionaven correctament.

S'hauran de seguir aquestes bones pràctiques:

L'estructura del test ha de dividir-se en les següents parts:

- **Inicialització:** inicialitzem l'entorn tal i com el necessitem per executar el test.
- **Execució:** executem les funcionalitats desitjades amb el flux adequat.
- **Validació:** validem que els resultats de l'execució coincideixen amb els resultats esperats.
- **Neteja:** eliminem el rastre d'execució del test.

Quan es comprova funcionalitats dependents de tercers (APIs, *webservices*, etc. és una bona pràctica l'ús de *mockups* per no afectar el sistema finalista.



10. PROPOSTA TÈCNICA

Els licitadors presentaran la seva oferta tècnica de realització del contracte tant per fer comprensible la seva proposta com per facilitar i fer possible la seva valoració d'acord amb els criteris d'adjudicació assenyalats en el plec de clàusules administratives particulars que regeixen per a aquesta contractació.

Cada licitador haurà de presentar la seva oferta en format electrònic, on tots els arxius han d'estar signats digitalment cadascun d'ells i en qualsevol dels formats admesos a la plataforma electrònica de conformitat amb l'establert al plec de clàusules administratives particulars.

Els licitadors poden adjuntar tota la informació complementària que considerin d'interès, tot i això hauran de presentar uns continguts mínims i la seva proposta haurà d'estar obligatòriament estructurada de la forma següent:

La proposta tècnica es presentarà en dos sobres electrònics; el sobre electrònic B, on s'inclourà la documentació que haurà de ser valorada segons els criteris de judici de valor assenyalats en les clàusules del plec de clàusules administratives particulars, i el sobre electrònic C, que haurà de contenir la documentació que haurà de ser valorada segons els criteris avaluable de forma automàtica assenyalats al plec de clàusules administratives particulars que regeix per aquesta contractació.

Es requereix utilitzar a l'oferta tipus de lletra Nimbus Roman, Liberation Sans, Calibri, Arial, Times New Roman o similar, de grandària 12 i interlineat simple.

10.1. Contingut sobre electrònic B

En el sobre electrònic B s'inclourà la següent documentació indexada de manera que faciliti la seva localització. El nombre màxim de pàgines entre tots els documents a presentar serà de **140**. No es tindran en consideració en la valoració aquelles pàgines que superin aquest màxim.

A nivell general i d'aplicació a tota la proposta tècnica, es valorarà l'enteniment del plec tècnic, de l'abast i el servei específic del contracte i la seva aplicació en millores i idees a aplicar sobre el servei. No es tindrà en consideració la còpia directa d'elements o apartats del plec tècnic, i es requereix que sigui específic per l'objecte del contracte, pels serveis descrits al plec tècnic i la seva tipologia, així com pel context de treball detallat (eines i procediments).

L'adjudicatari haurà de presentar la seva proposta tècnica seguint el següent ordre:

1. Plantejament general

Ha d'exposar l'enteniment del servei que s'ha de prestar i les línies principals de l'estratègia per dur-lo a terme i l'esquema de l'equip del treball indicant el percentatge de dedicació (*) i la seva organització, tenint en compte els requeriments exposats en el plec de prescripcions tècniques. Es detallarà tot el que es consideri interessant respecte



a les metodologies de treball emprades. Inclourà un resum executiu de la proposta amb els esquemes i aspectes clau que es considerin.

(*) en el percentatge de dedicació no es podrà indicar ni evidenciar cap de les millores avaluables de forma automàtica

2. Serveis Transversals de Manteniment

2.1. Reporting

Els Informes de Seguiment proposats han de millorar els mínims descrits en el present plec, especialment el contingut i format mínims previstos i detallats al plec de prescripcions tècniques.

2.2. Suport

Ha d'incloure els diagrames de flux i procediments associats que incloguin els mínims descrits en el present plec incloent la visió, estructura i relacions dels serveis de Help Desk, SAU, suport funcional i suport tècnic.

2.3. Coordinació entre serveis del contracte

Ha d'incloure la proposta d'enfocament per garantir la coordinació dels serveis d'aquest contracte de manteniment en el que respecta a l'organització dels serveis de manteniment correctiu, de manteniment recurrent, evolutius recurrents, serveis transversals de manteniment, i aprovisionament de la infraestructura, que permeti la coordinació d'equips aplicable a tots els serveis/aplicacions i un control i seguiment eficient

2.4. Pla de Qualitat del Servei

Ha d'incloure la proposta de Pla de Qualitat del Servei, respectant els mínims establerts a l'apartat 7 del plec de prescripcions tècniques, que permeti la valoració de la seva viabilitat, coherència, realisme i estructura organitzativa, incloent els mecanismes que garanteixin l'execució del servei amb la qualitat estipulada i els procediments que assegurin la traçabilitat entre les aplicacions i la seva documentació associada actualitzada d'acord amb els canvis o peticions realitzades al llarg del cicle de vida del servei de manteniment i la traçabilitat amb el codi associat.

2.5. Pla de Transició i Procediment de recepció de la infraestructura

Ha d'incloure la proposta d'un model organitzatiu de la transició del servei (detallant especialment el procés de la recepció del servei, al considerar que és més crític i previsible que el procés de devolució), respectant els mínims establerts l'apartat 3.2.9 del plec de prescripcions tècniques, que permeti assegurar una eficient transició de tots els serveis d'aplicacions i garantir la continuïtat dels serveis de contracte.

En aquesta secció, el licitador explicarà el procés que articularà per a la recepció del servei, detallant correctament les tasques a dur a terme, i concretant la transferència de coneixement dels treballs previstos en el contracte i l'inici de la responsabilitat del servei (veure apartat **3.2.9** Transició, i en concret: **3.2.9.2** Tasques rellevants de recepció del servei).



3. Propostes tècniques de millora de la infraestructura i el servei

Els licitadors han de presentar les propostes tècniques d'evolució de la plataforma, d'acord amb les necessitats plantejades en el present plec i a la clàusula de "Criteris de valoració de les ofertes" del plec de clàusules administratives particulars.

Caldrà exposar cadascuna de les propostes demanades en apartats independents, seguint el mateix ordre dels criteris de valoració que s'indiquen en el plec de clàusules administratives particulars.

A l'annex 1 i 2 es detalla la infraestructura actual i la volumetria del servei. I en concret a l'apartat 13.3 "reptes d'evolució de la infraestructura" es dona més informació de context per tal de que el licitador pugui fer propostes de millora. Es demanen propostes sobre aquests temes:

- Automatització
 - Recuperació automàtica dels webs
 - Infraestructura com a codi (iaaC)
 - Autoprovisionament
- DevOps
 - Eines de control de desplegament ..
 - Eines de descobriment i gestió d'inventari de versions / d'estat del web
- Projectes
 - Aplicatiu d'Arxiu històric de Webs
 - Aplicatiu de gestió de cues (puntual, sota demanda)
 - Aplicatiu per mantenir al dia les versions globals, dur a terme actualitzacions massives, gestionar les polítiques de seguretat
 - Suport intern per Intel·ligència Artificial
- Robustesa
 - Evolució de clúster d'aplicacions
 - Contingència
 - Contenedors i plataforma Kubernetes
 - Còpies de seguretat
- Seguretat
 - Securitització de la infraestructura
 - Securitització de webs LAMP
 - Protocol d'aplicació d'actualitzacions massives crítiques
 - Protocol de resposta a possible intrusió/infecció d'un web o sistema
 - Govern de certificats digitals .
- Infraestructura
 - Infraestructura destí
 - Optimització de costos

10.2. Contingut sobre electrònic C

En el sobre electrònic C s'inclourà la documentació que s'especifica en el plec de clàusules administratives particulars.



11. CONDICIONS GENERALS D'EXECUCIÓ

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.

Els estàndards vigents aprovats i operatius del cos normatiu establerts es troben recollits sota la nomenclatura de "Criteris de Seguretat de la informació i Protecció de Dades" i es troben a disposició dels licitadors sota demanda. El proveïdor haurà d'aplicar aquestes normatives i estàndards que li corresponguin per l'abast del contracte i donar compliment a les modificacions dels estàndards o a aquells de nova creació.

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 del REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, així com de la resta de l'ordenament jurídic que sigui d'aplicació.

Pel que 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 que 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 que fa referència a la protecció de dades de caràcter personal (LOPDGDD).

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.

11.1. 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.
- Assegurar que tot el personal del proveïdor que hagi de tractar dades o sistemes de tractament de dades de nivell sensible o superior signin un Acord de Confidencialitat Individual. L'IMI es reserva el dret d'auditar aquest aspecte.
- 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.

11.2. 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.

11.3. Auditoria

L'IMI auditarà que l'adjudicatari vetlli per la qualitat 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 a 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.

11.4. Gestió d'Incidents de Seguretat

L'adjudicatari, sempre que sigui possible mitjançant el responsable de seguretat, informarà a Departament de Seguretat de l'IMI, de qualsevol incident de seguretat, ja tingui afectació al sistema d'informació de Vincles com a infraestructura o sistemes que l'adjudicatari empli en la prestació del servei objecte del present contracte, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert pel Departament de Seguretat de l'IMI.

L'adjudicatari ha de disposar d'un procediment de notificació i gestió d'incidents de seguretat, on es registrin tots els incidents de seguretat que es produeixin.

L'adjudicatari col·laborarà amb el Departament de Seguretat de l'IMI en la resolució de qualsevol incident produït en el seu entorn, i que afecti als sistemes d'informació o a les dades subjectes a l'aplicació del present contracte, proporcionant totes les evidències requerides.

En cas que l'incident afecti els sistemes i els recursos propietat de l'adjudicatari, serà responsabilitat d'aquest realitzar les accions de contenció i resolució necessàries per restaurar el servei.

L'adjudicatari haurà de documentar els incidents de seguretat i indicar el tipus d'incidència, moment en que es produeix, moment en que s'ha detectat, persona que fa la notificació, a qui es comunica, els efectes d'aquesta, moment en que se soluciona, descripció de la solució i persona que ho realitza. A l'esmentat registre s'han d'establir, a més, els procediments



realitzats de recuperació de la informació, persona que executa el procés i la informació restaurada.

La documentació d'un incident de seguretat de la informació i la investigació i resposta consegüent s'han de preparar mitjançant informes de forma cronològica i lliurar-se a al Departament de Seguretat de l'IMI, en el cas que hi hagi hagut afectació al servei prestat.

El Departament de Seguretat de l'IMI farà un seguiment periòdic de l'estat de la resolució dels incidents, i l'adjudicatari es comprometrà a respondre amb els informes que li siguin sol·licitats.

11.5. Confidencialitat

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

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

11.6. Dimensionament/gestió de capacitats

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

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

11.8. 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.

11.9. Control d'accés

11.9.1. 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.
- S'informarà a l'usuari de l'últim accés efectuat amb la seva identitat.

11.9.2. 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.

11.10. Gestió del Personal

11.10.1. Deures i obligacions del personal

El/La 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/La 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/La 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 pertogui 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/La 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'Acord de confidencialitat i compliment de polítiques de seguretat per a treballadors externs amb accés a informació de l'Ajuntament de Barcelona" (Plantilla CONTRACTE DE CONFIDENCIALITAT PERSONAL EXTERN) serà signat per l'empresa adjudicatària i lliurat al Cap de Projecte de l'Ajuntament. El document d'acceptació de les obligacions signat per les persones adscrites a l'execució d'aquest contracte serà presentat 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.

11.10.2. 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.

11.11. 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.

11.12. Protecció del lloc de treball

11.12.1. 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.

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

11.12.2. Bloqueig del lloc de treball

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

11.12.3. 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.

11.12.4. Medis alternatius

L'adjudicatari garantirà l'existència i disponibilitat de mitjans alternatius de tractament de la informació per al cas que fallin els mitjans habituals. Aquests mitjans alternatius hauran d'estar subjectes a les mateixes garanties de protecció. Igualment, s'haurà d'establir un temps màxim perquè els equips alternatius entrin en funcionament.

11.13. Protecció dels Suports Informàtics

L'adjudicatari haurà de gestionar els suports informàtics amb informació de l'Ajuntament de Barcelona seguint les següents pautes.

11.13.1. 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.

11.13.2. Criptografia



Qualsevol informació corporativa que requereixi ser xifrada a la seva ubicació d'emmagatzemament, en particular a tots els dispositius extraïbles del tipus CD, DVD, discos USB, o uns altres de naturalesa anàloga, han de seguir els estàndards de seguretat, custòdia i protecció de les claus establerts per IMI-Seguretat.

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

11.13.3. Transport

L'adjudicatari garantirà que els dispositius romanen baix 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.

11.13.4. Esborrat i destrucció

En aquells casos que apliquin, que seran prèviament avisats per l'Ajuntament, 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. S'hauran de destruir de forma segura els suports en cas que la naturalesa del suport no permeti un esborrat segur o quan així ho requereixi el procediment associat al tipus d'informació continguda, fent us dels productes certificats per l'IMI.

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.

11.14. Protecció de la Informació

11.14.1. 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.



11.14.2. Protecció del correu electrònic

En el cas 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.

11.15. 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.

11.16. 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 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.

11.17. Protecció de dades de caràcter personal

L'adjudicatari, com a encarregat de tractament i tenint en compte l'adequació del nivell de seguretat al risc, tindrà les obligacions següents:

- Utilitzar les dades personals objecte del tractament, o les que reculli per a la seva inclusió, només per a la finalitat objecte d'aquest encàrrec. En cap cas podrà utilitzar-les per a finalitats pròpies.
- Tractar les dades personals seguint únicament les instruccions documentades del responsable.
- Portar, per escrit, un registre de totes les categories d'activitats de tractament efectuades per compte del responsable que contingui:
 - El nom i les dades de contacte de l'encarregat o encarregats i de cada responsable per compte del qual actuï l'encarregat.
 - Les categories de tractaments efectuades per compte de cada responsable.
 - Una descripció general de les mesures tècniques i organitzatives de seguretat apropiades que estigui aplicant.
- No comunicar dades a terceres persones, excepte en el cas que compti amb l'autorització expressa del responsable del tractament, o en els supòsits legalment admissibles. Si l'encarregat vol subcontractar, haurà d'informar obligatòriament al responsable i sol·licitar la seva autorització prèvia.
- Mantenir el deure de secret respecte a les dades de caràcter personal a les quals hagi tingut accés en virtut del present encàrrec, inclús després de que finalitzi el contracte.
- Garantir que les persones autoritzades al tractament de dades personals s'hagin compromès, de forma expressa i pe escrit, a respectar la confidencialitat i a complir les mesures de seguretat corresponents, de les quals se les ha d'informar convenientment.
- Mantenir a disposició del responsable la documentació acreditativa del compliment de l'obligació establerta a l'apartat anterior.
- Garantir la formació necessària en matèria de protecció de dades personals de les persones autoritzades per a tractar dades de caràcter personal.
- Quan les persones afectades exerceixin els drets reconeguts per la normativa de protecció de dades davant de l'encarregat del tractament (accés, rectificació, supressió, oposició, limitació del tractament i portabilitat de les dades), aquest haurà de comunicar-ho per correu electrònic a l'adreça que indiqui el responsable. La comunicació haurà de fer-se de forma immediata i en cap cas més enllà del dia laborable següent al de la recepció de la sol·licitud, juntament amb altres informacions que puguin ser rellevants per a resoldre la sol·licitud (per valorar la pertinença del seu contingut)



- Assistir al responsable en la seva obligació de respondre a les sol·licituds que tinguin per objecte l'exercici dels drets dels interessats així com també als requeriments de les autoritats de control.
- En allò referent a les notificacions de violacions de la seguretat de les dades:
 - L'encarregat del tractament notificarà al responsable del tractament, de forma immediata i mitjançant l'adreça de correu electrònic facilitada pel responsable, les violacions de la seguretat de les dades personals al seu càrrec de les quals tingui coneixement, juntament amb tota la informació rellevant per a la documentació i comunicació de la incidència.

Es facilitarà, com a mínim, la informació següent:

1. Descripció de la naturalesa de la violació de la seguretat de les dades personals, incloent quan sigui possible, les categories i el nombre aproximat d'interessats afectats i les categories i el nombre aproximat de registres de dades personals afectats.
2. Dades de la persona de contacte per obtenir més informació.
3. Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals. Descripció de les mesures adoptades o proposades per a posar remei a la violació de la seguretat de les dades personals, incloent si escau, les mesures adoptades per a mitigar els possibles efectes negatius.

Si no és possible facilitar la informació de forma simultània, la informació s'ha de facilitar de forma gradual i sense dilacions.

- L'Encarregat, a petició del responsable, comunicarà en el menor temps possible aquestes violacions de la seguretat de les dades als interessats, quan sigui probable que la violació suposi un alt risc pels drets i llibertats de les persones físiques.

La comunicació ha de fer-se en un llenguatge clar i senzill i haurà d'incloure els elements que en cada cas assenyali el responsable, com a mínim:

1. La naturalesa de la violació de les dades.
2. Dades del punt de contacte del responsable o de l'encarregat on es pugui obtenir més informació.

- Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals.
- Descripció de les mesures adoptades o proposades pel responsable de tractament per a posar remei a la violació de la seguretat de les dades personals, incloent si escau, les mesures adoptades per a mitigar els possibles efectes negatius.
- Posar a disposició del responsable tota la informació necessària per a demostrar el compliment de les seves obligacions, així com per a la realització



de les auditories o les inspeccions que realitzi el responsable o un altre auditor autoritzat per ell.

- Permetre i contribuir a la realització d'auditories, incloses inspeccions, per part del responsable o auditor autoritzat per aquest.
- D'acord amb l'art. 32 del RGPD i el nivell de mesures establert per l'Ajuntament de Barcelona, prendrà totes les mesures necessàries per a la seguretat del tractament, incloent entre d'altres, si s'escau:
 - La pseudoanonimització i el xifrat de dades personals.
 - La capacitat de garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament.
 - La capacitat de restaurar la disponibilitat i l'accés a les dades personals de forma ràpida en cas d'incident físic o tècnic.
 - Un procés de verificació, avaluació i valoració regulars de l'eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament.
- Per tal d'avaluar l'adequació del nivell de seguretat, tindrà particularment en compte els riscos que presenti el tractament de les dades com a conseqüència de la destrucció, pèrdua o alteració accidental o il·lícita de dades personals trameses, conservades o tractades d'altra forma, o la comunicació o accés no autoritzats a les dades esmentades.
- Al finalitzar la prestació dels serveis del tractament d'acord amb les instruccions que rebí de l'Ajuntament de Barcelona, suprimir o tornar totes les dades personals i suprimir les còpies existents (tret que existeixen obligacions legals que requereixin la conservació per un temps definit).
- Si considera que una instrucció del responsable infringeix el RGPD o altres disposicions en matèria de protecció de dades de la Unió o dels Estats membres, l'encarregat informarà immediatament al responsable.
- Si l'encarregat infringeix la normativa de protecció de dades vigent (RGPD, LOPDGDD...) serà considerat responsable del tractament.

En cas que l'encarregat de tractament decideixi recórrer a un altre encarregat (com per exemple, en cas de subcontractació):

- Haurà de comptar amb l'autorització prèvia per escrit de l'Ajuntament de Barcelona.
- Si s'autoritza recórrer a un altre encarregat i s'hagués de produir algun canvi, s'haurà d'informar a l'Ajuntament de Barcelona, i aquest tindrà la possibilitat d'oposar-se i rescindir el contracte.
- L'altre encarregat tindrà les mateixes obligacions de protecció de dades que les estipulades en el contracte o acte jurídic entre el responsable i l'encarregat i la consideració d'encarregat de tractament de l'Ajuntament de Barcelona.
- Si l'altre encarregat incompleix les seves obligacions de protecció de dades, l'encarregat inicial seguirà sent plenament responsable davant de l'Ajuntament de Barcelona pel que respecta al compliment de les obligacions de l'altre encarregat.

11.18. Conformitat amb l'Esquema nacional de seguretat



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

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

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

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

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

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

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



12. CLÀUSULES GENERALS DE SEGURETAT

12.1. Clàusules d'administració de producte

12.1.1. Gestió d'identitats, autenticació d'usuaris

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

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

Autenticació interna

Els usuaris interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per l'IMI basats en protocols estàndards de seguretat. L'empresa proveïdora haurà d'assegurar que s'utilitzi el proveïdor d'identitats corporatiu (en endavant IDP) per a l'autenticació dels usuaris. La solució IDP utilitzada per l'IMI és el Reg Hat Single Sign On (RH-SSO)

La integració amb RH-SSO 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

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.

12.1.2. Autorització dels usuaris als sistemes

L'IMI disposa d'un repositori centralitzat d'autoritzacions dels usuaris corporatius, basat en un directori actiu, que és d'on l>IDP corporatiu recull les autoritzacions. 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 (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.

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 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.

12.1.3. 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.

12.1.4. 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.



12.1.5. Manteniment

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

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

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

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

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

12.1.6. Xifratge de dades

Qualsevol informació corporativa que requereixi ser xifrada en la seva ubicació d'emmagatzemament (i per tant, queda exclòs l'encriptació per transit en les comunicacions) ha de seguir els estàndards de seguretat i la custòdia i protecció de les claus estableix el Departament de Seguretat de l'IMI.



El Departament de Seguretat de l'IMI ha de assegurar la disponibilitat de la informació als propietaris d'aquesta dins de l'Ajuntament. El Departament de Seguretat de l'IMI custodiarà les claus de xifratge.

12.1.7. Certificats

El Departament de Seguretat de l'IMI serà el responsable de la custòdia i protecció dels certificats digitals emesos en nom de l'Ajuntament de Barcelona a través de del Departament de Seguretat de l'IMI. 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 el Departament de Seguretat 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.

12.1.8. Antimalware

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

L'IMI seguretat tindrà accés en consulta a la consola de gestió d'aquests programaris del proveïdor.

12.1.9. 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 i 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.

A banda de ser responsable de la generació de les còpies de seguretat, l'adjudicatari serà responsable de garantir que aquestes són perfectament funcionals, per mitjà de la realització d'exercicis periòdics de recuperació de backups. Els exercicis han de poder donar cobertura a tots els actius sota el present contracte dins d'un termini màxim d'1 any.

12.1.10. 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.

12.1.11. Explotació

Gestió de la configuració

L'adjudicatari s'encarregarà de gestionar de forma contínua 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.

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.

Protecció de claus criptogràfiques

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

12.1.12. Protecció dels serveis

Protecció enfront de la denegació de servei

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

- Es planificarà i dotarà al sistema de capacitat suficient per atendre a la càrrega prevista sense posar en risc la disponibilitat del sistema.

Es desplegaran tecnologies per prevenir els atacs coneguts.

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 obviat 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 d'URL.
 - Es previndran atacs de manipulació de fragments de la informació que s'emmagatzemin en el disc dur del visitant d'una pàgina web a través del seu



navegador, a petició del servidor de la pàgina, 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.

12.2. Clàusules de desenvolupament de producte

12.2.1. Clàusula de propietat intel·lectual

La propietat intel·lectual dels treballs realitzats a l'empareda d'aquest contracte pertany a l'Ajuntament de Barcelona de forma exclusiva. Els productes o subproductes derivats, no podran ser utilitzats sense la deguda autorització prèvia.

L'accés a informació i/o productes protegits per la propietat intel·lectual, propietat de l'Ajuntament de Barcelona, necessaris per al desenvolupament del producte o servei contractat no pressuposa en cap cas la cessió de la mateixa.

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.

12.2.2. 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 al llarg de tot el cicle de vida, incloent normes de programació segura.

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 de les anàlisis hauran de ser acordats conjuntament amb el responsable del contracte. El software emprat a l'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'anàlisi d'imatges Docker. La tecnologia emprada a l'IMI i la preferent d'ús per part de l'adjudicatari és Coreos Clair.

En cas d'emprar softwares diferents als plantejats anteriorment, hauran de ser comunicats i justificats degudament al responsable del contracte.

12.2.3. 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.

Adicionalment, l'adjudicatari realitzarà les següents inspeccions prèvies a l'entrada en servei:

- Anàlisi de vulnerabilitats.
- Test de penetració.

12.2.4. 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.

12.2.5. 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 vàlides 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 per IMI-Seguretat. En tot cas s'ha de complir la política de signatura electrònica de l'Ajuntament de Barcelona.

12.2.6. 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.

12.2.7. Informe de seguretat

El proveïdor elaborarà a petició de seguretat un informe on es detallaran tots els aspectes rellevants sobre Seguretat del seu contracte.

L'estructura d'aquest informe incloent la informació requerida es lliurarà al proveïdor durant les primeres etapes del contracte.

12.3. Seguretat sistemes d'informació

Clàusules d'allotjament de sistemes:

12.3.1. Àrees separades i control d'accés



L'adjudicatari garantirà que els elements de la infraestructura s'ubicaran en àrees específiques per a la seva funció. Aquestes àrees estaran dotades d'un perímetre de seguretat de tal forma que únicament s'hi pugui accedir per les entrades previstes i vigilades.

12.3.2. Identificació de persones

El mecanisme de control d'accés disposarà dels següents requeriments mínims:

- S'identificaran totes les persones que accedeixen als locals on hi ha equipament que formi part dels sistemes de l'Ajuntament.
- Es registraran les entrades i sortides de persones.

12.3.3. Condicionament dels espais

Els espais on s'ubiquen els sistemes d'informació i els seus components, disposaran dels elements adequats per al funcionament eficaç de l'equipament instal·lat, en especial:

- Condicions de temperatura i humitat.
- Protecció en front a amenaces identificades per l'adjudicatari.
- Protecció del cablejat front a incidents.

12.3.4. Energia elèctrica

Els locals on s'ubiquin els sistemes d'informació i els seus components disposaran de subministrament elèctric i les escomeses necessàries per al seu funcionament, de forma que:

- Es garanteixi el subministrament de potència elèctrica.
- Es garanteixi el correcte funcionament de llums d'emergència.

12.3.5. Protecció contra incendis

Els locals on s'ubiquin els sistemes d'informació i els seus components es protegiran contra incendis aplicant la normativa industrial corresponent.

12.3.6. Registre d'entrada i sortida d'equipament

L'adjudicatari garantirà que es mantingui un registre d'entrada i sortida de qualsevol equipament dels locals, identificant també a la persona que autoritza el moviment.

12.3.7. Seguretat del perímetre

L'adjudicatari haurà de disposar d'un tallafocs que separi la xarxa interna del exterior. Tot el trànsit de dades ha de ser filtrat per aquest tallafocs per deixar pas només a les comunicacions legítimes i autoritzades, havent de configurar la solució de seguretat acuradament per garantir-ho.

12.3.8. Protecció de les comunicacions

En relació al establiment de comunicacions entre l'adjudicatari i l'Ajuntament de Barcelona, s'hauran de garantir un requisits mínims de seguretat atenent qüestions de autenticitat i integritat:



- S'ha de garantir la autenticitat de la comunicació abans de realitzar l'intercanvi d'informació.

S'han de prevenir atacs actius amb la posterior activació dels plans per a gestió d'incidents. Com a atacs actius es considerarà l'alteració de informació en trànsit, la injecció de informació no legítima i el segrest de la sessió.



13. ANNEX 1 INFRAESTRUCTURA WEB

13.1. Catàleg d'aplicacions

A continuació es troben classificats els serveis i aplicacions del contracte:

Codi Servei	Nom Servei	Nom Aplicació
SER0188	Infraestructures web	<p><u>A CIUTADÀ: Aplicacions de servei dins contenidors</u> Com s'hi va (kubernetes) com-shi-va.barcelona.cat Cercador de les webs: cercador.barcelona.cat (Python/Django) BIMA Barcelona imatges: imatges.barcelona (Python/Django) Estatificador de fitxers de NASIA (per web mercè) Gestor ubicació cavalcada reis Nadal Cercador de residus (backoffice i API) Repositori documentació procediments interns («Druida») Gestor barres corporatives («Nlron») Transparència: Subvencions i Retribuscions ("Subconv") Web central Notícies: Infobarcelona.barcelona.cat (Python/Django) Gestor de xarxes socials («Moderador-xs») Bcn-llibres (backoffice) mapaciutatdigital (mapa per web ciutatdigital) (Python/Django) Gestió inventari versions aplicacions mòbils («Palàntir») Gestor d'enllaços trencats («spider-web») (Python/Django)</p> <p><u>Altres aplicacions backoffice</u> IBE aplicacions (Python Django dockeritzades). Transparència: API Who-is-Who (Python/Django) OSAM, pipelines de construcció d'aplicacions mòbils (Jenkins, scripts) CATB</p> <p><u>Aplicacions per us de desenvolupadors o gestió de la plataforma</u> Sygox (Flask + React) per govern d'entorns LAMP, 1050 entorns i 300 desenvolupadors. GitLab (community edition) amb 1050 repositoris de codi, 400 usuaris i un runner per desplegament de CI/CD Secrets, enviament de secrets efímers amb OneTimeSecret Logger, consolidació de traces amb syslog-ng Grafana i Influxdb per emmagatzematge i mostrat de mètriques sistema CheckMK per monitorització de sistemes SSHail Bastion per exposar servei de SSHail a l'exterior. Sentry per recol·lectar i mostrar traces a desenvolupadors LDAP extern, gestió de LDAP central per aplicacions externes phppackages repositori de paquets PHP</p> <p><u>A CIUTADÀ: Webs CMS</u> 538 Web CMS Estàndard 57 Web CMS Estratègica</p>

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.



13.2. Descripció infraestructura cloud públic AWS

13.2.1. Introducció Plataforma Hostlamp

La plataforma HOSTLAMP es aquella que allotja les webs públiques informatives (sense tràmits ni dades d'usuari) de l'Ajuntament de Barcelona.

Tips d'aplicacions

Per la naturalesa informativa principalment per CMS desenvolupats en PHP com Drupal i Wordpress per tal de facilitar la introducció de continguts a les persones que els administren. Aquestes aplicacions se les coneix com els PHP consolidats i superen el miler d'entorns, les quals aproximadament 600 son productius.

A banda també existeixen altres aplicacions més diverses que varien entre eines d'ús intern, serveis transversals de les webs o senzillament aplicacions no PHP. Dins d'aquest bloc trobem aplicacions Python / Django o d'altres completament diverses. Aquestes aplicacions estan dockeritzades i desplegades tant a servidors individuals com clústers Kubernetes.

La plataforma està molt orientada a esdeveniments per la qual cosa hi poden haver pics significatius de manera periòdica i estacional com podria ser per La Mercè. També tenim pics imprevistos per esdeveniments que succeeixen a la ciutat com son emergències i esdeveniments que podem preveure com promocions de campanyes polítiques.

Infraestructura

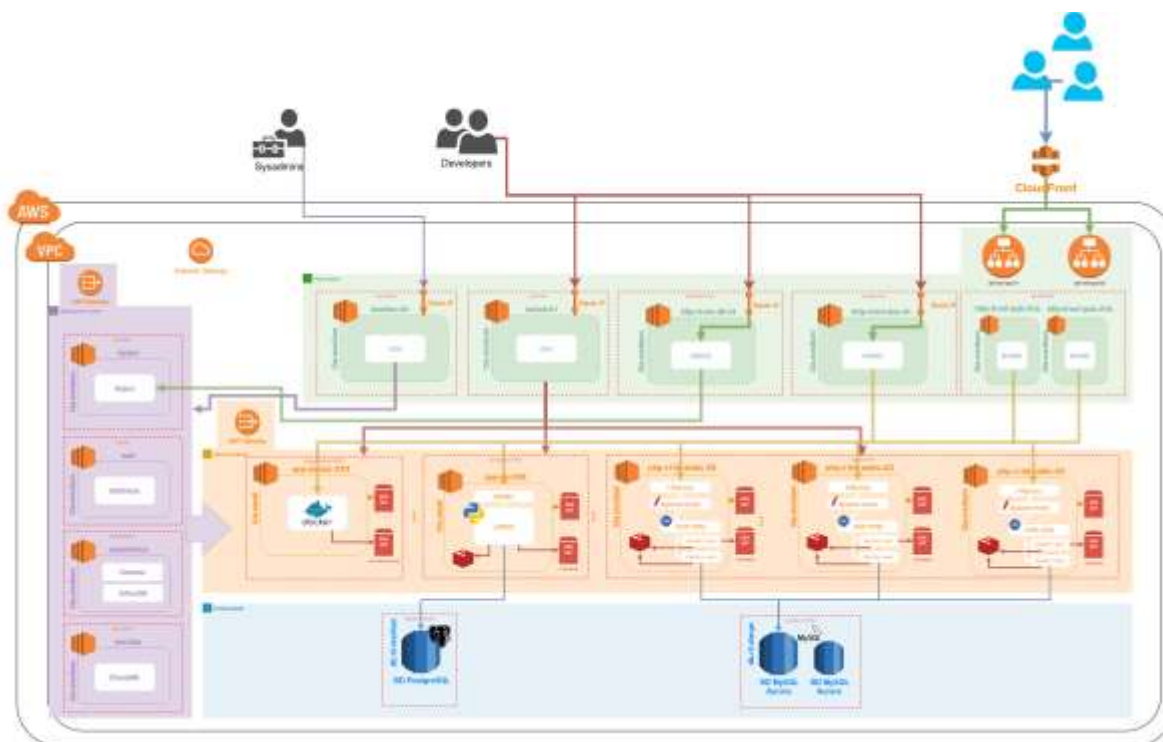
La infraestructura està majoritàriament allotjada a cloud públic d'AWS i governada emprant infraestructura com a codi. Terraform per la part de Cloud i SaltStack per la configuració i aprovisionament de servidors.

Per facilitar la gestió de la plataforma tant per els administradors, tècnics de l'Ajuntament i desenvolupadors de les aplicacions s'empra l'eina *Sygox*, un portal intern de desenvolupadors (IdP) que governa i administra les aplicacions PHP consolidades. Totes les accions sobre aplicacions PHP (creació, accessos, obtenció de credencials, comprovacions, integració amb repositoris, gestió de crons etc.) es fa mitjançant el *Sygox* que alhora dispara accions amb SaltStack o les seves integracions amb AWS.

Les peticions dels usuaris entren per els dominis de l'Ajuntament, la majoria dels quals tenen configurada la CDN de CloudFront per fer cache de resultats i optimitzar rendiment.

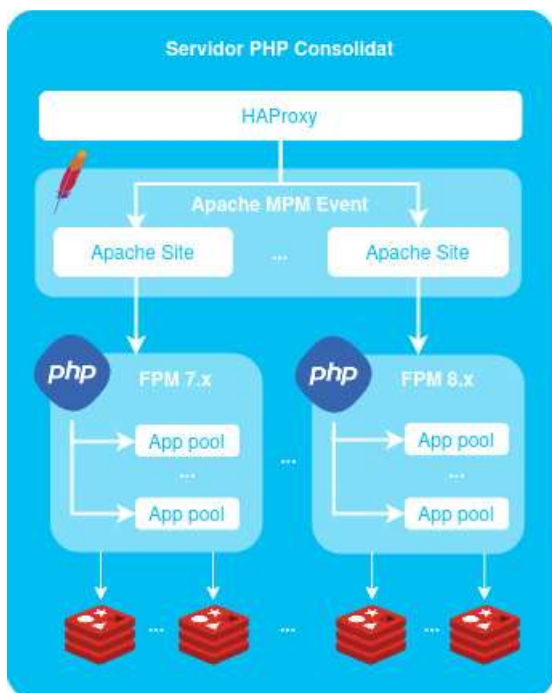
La CDN envia el trànsit als balancejadors públics que deriven les peticions als frontal NGINX que enrutaran les peticions al servidor corresponent. S'empra una doble capa de balancejadors de AWS (ALBs) i NGINX ja que el nombre de regles d'enrutat (milers) supera els límits dels ALB de AWS. Les regles NGINX dels frontals estan governades amb SaltStack.

Veure resum de les tecnologies a l'apartat 4.5.1.



Detall tècnic de les aplicacions PHP

Els servidors d'aplicacions PHP contenen les aplicacions separades per usuaris UNIX. Cada aplicació disposa d'un usuari de sistema, un site de Apache, un pool de PHP-FPM i un Redis. Les peticions entren al servidor per un HAproxy, aquest les deriva a un site de Apache escoltant a un port TCP concret, l'Apache serveix els fitxers estàtics i avalua els .htaccess per finalment derivar-ho emprant un UNIX socket al pool de PHP-FPM concret que executarà l'aplicació. El PHP té a la seva disposició un Redis on s'hi connecta per UNIX socket així com accés a una base de dades MySQL allotjada sobre un clúster Aurora.

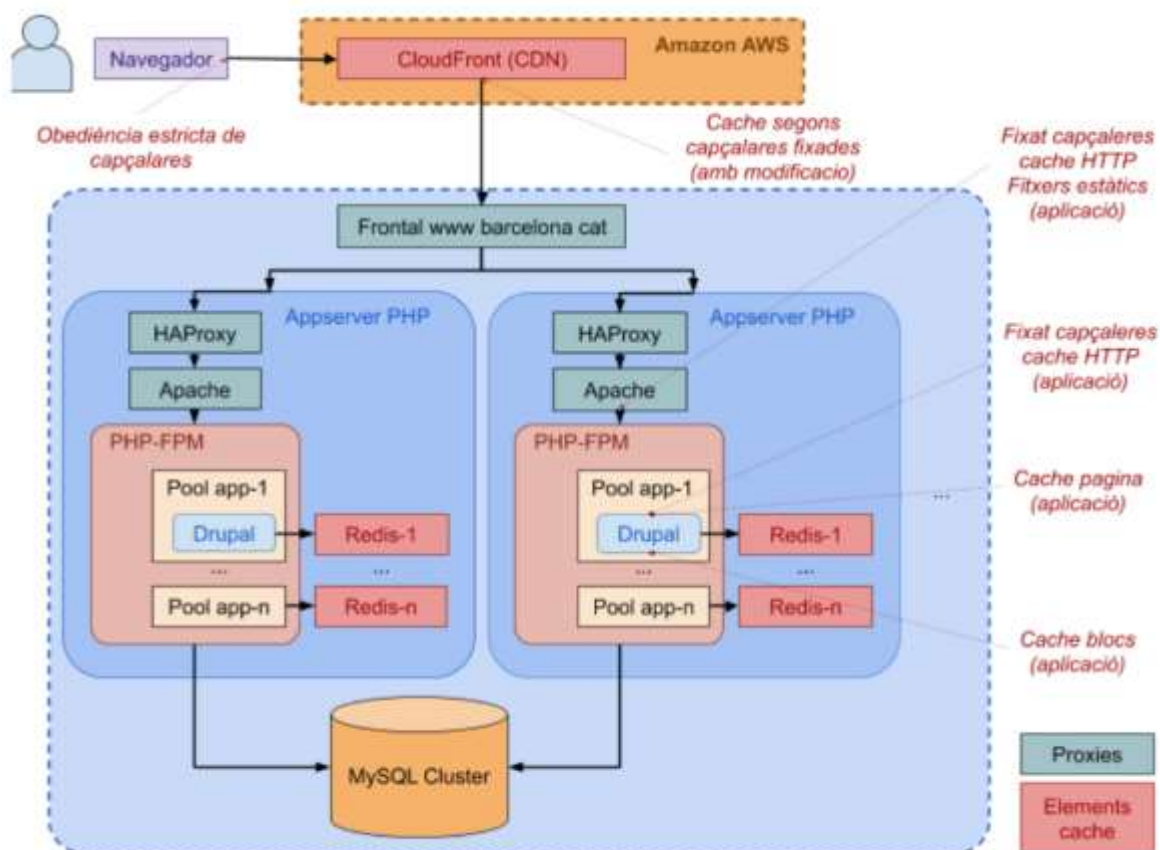


El número d'aplicacions PHP per servidor varia en funció de les peticions que es reben. La regla manual es que per cada 150 peticions per minut hi ha d'haver una CPU.

Les instàncies tipus t3a.large son suficients per allotjar 80 aplicacions tipus.

Aplicacions de molt trànsit com les Home ajuntament.barcelona.cat o www.barcelona.cat i guia.barcelona.cat tenen una sola instància per les tres.

Per evitar problemes de latència amb NFS totes les aplicacions fan ús de disc local. Donat que les aplicacions consolidades no son "12 factor" l'ús de disc local fa que no puguin tenir alta disponibilitat ta nivell de servidor. Si que hi ha sistemes de recuperació ràpida de l'aplicació i el servidor per tal de minimitzar downtime en cas d'incident. Si que estan redundants i en alta disponibilitat els elements comuns entre les aplicacions com son els frontals / balancejadors i clústers de bases de dades.



El flux de les aplicacions no PHP com les Python Django tenen una arquitectura similar però les peticions en lloc d'anar a un servidor amb LAMP van a un que conté docker i on allà els Dockerfiles i docker-compose que hagi especificat el desenvolupador ja s'encarrega de servir l'aplicació.

Per tal de facilitar la feina als desenvolupadors i tècnics existeixen scripts de comprovació (checklist) per comprovar els errors típics d'aplicacions i així poder minimitzar errors en les publicacions de noves webs.

De la mateixa manera existeix un wiki de documentació per els procediments tant de l'administració de la plataforma com de l'ús d'eines com Sygox i la manera de desplegar i desenvolupar els CMS.

13.2.2. Justificació de la migració al cloud a AWS

Durant l'execució de de l'anterior contracte i complint amb la previsió de millora tècnica del plec es va migrar la infraestructura des del proveïdor de cloud anterior, DigitalOcean, a Amazon Web Services (AWS).

El canvi de proveïdor va venir motivat per tenir serveis que permetessin millor control de xarxes, seguretat i garantia de disponibilitat.

Aquesta migració va venir motivada per poder:



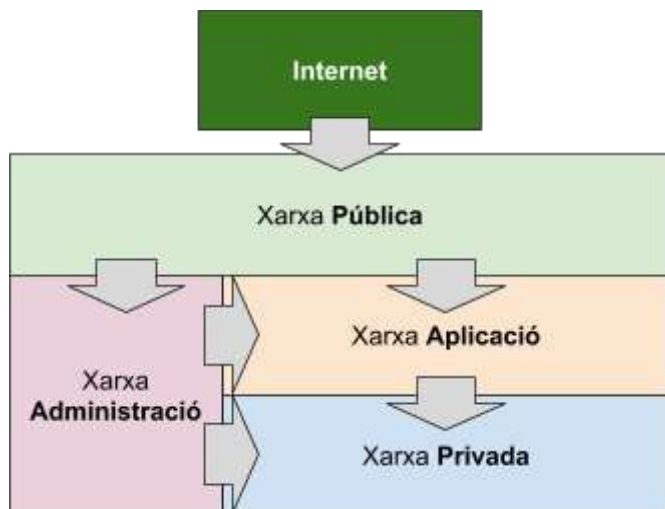
- Emprar serveis gestionats oferts a AWS, com ara Bases de Dades o NFS, reduint el cost en operativa i incrementant la disponibilitat del servei.
- Emprar Xarxes Privades Virtuals (VPC) per definir segments de xarxa i reduir l'exposició a Internet de la infraestructura.
- Emprar Grups de Seguretat (*Security Groups*) per tenir una capa addicional de tallafocs als serveis i servidors.
- Emprar *AWS Shield* per poder posar un tallafocs d'aplicació web (WAF) a tota la infraestructura.
- Aprofitar la migració per fer neteja de configuracions obsoletes.
- Aprofitar la migració per definir millors plans de contingència.

Amb la migració és va passar a emprar un proveïdor al núvol més robust en tots els sentits assolint millor nivell de disponibilitat i seguretat.

13.2.3. Arquitectura de xarxa

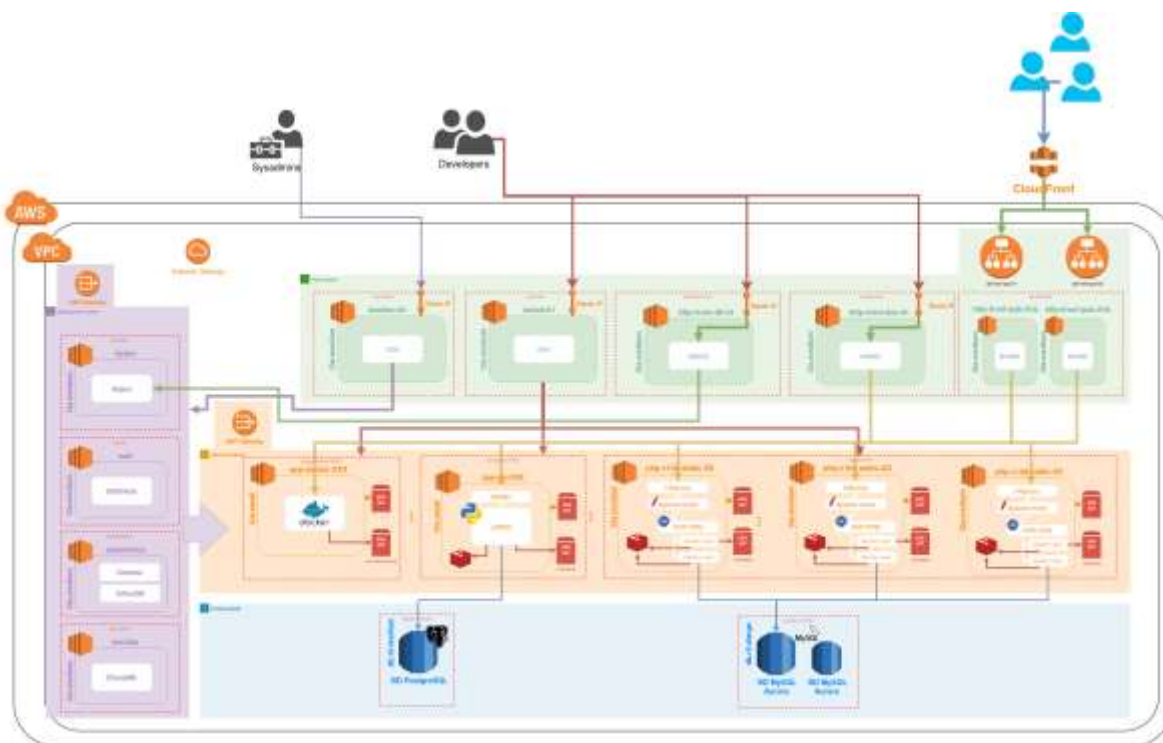
L'arquitectura està basada en Xarxes Privades Virtuals (VPC) i es divideix en 4 sub-xarxes:

- **Xarxa pública:** Permet trànsit tant d'entrada com de sortida a internet. Els serveis desplegats a aquesta xarxa disposen d'IP pública. És on s'hi desplegen els frontals o serveis de bastió.
- **Xarxa aplicació:** Només permet trànsit de sortida a internet. Els serveis no tenen IP pública i només accepten trànsit d'instàncies o serveis de la *xarxa pública*. No s'hi pot accedir directament des de internet. És on s'hi desplegen els servidors d'aplicacions.
- **Xarxa privada:** No permet trànsit entrant ni sortint a internet. Els serveis només accepten connexions de servidors de la *xarxa d'aplicació*. És on hi ha les bases de dades i serveis d'emmagatzematge.
- **Xarxa administració:** Té sortida a Internet. L'accés només és possible emprant VPN o bé instàncies de bastió de la *xarxa pública*. És la xarxa emprada per desplegar eines de govern i monitorització.



El detall de les VPCs està explicat més endavant al punt de Millores de Seguretat - Arquitectura basada en VPCs

L'arquitectura es pot resumir en el següent diagrama:



En el diagrama es veu la interacció entre els quatre grups d'aplicacions, que entrem a definir més profundament a continuació.

En la **xarxa pública** trobem diferents tipus de serveis:

- **Frontals:** Servidors que reben les peticions dels usuaris. El frontal té la funció de centralitzar totes les peticions i de forma transparent les fa arribar a diferents



servidors d'aplicacions (que es troben a la xarxa d'aplicació).

- **Bastió:** Servidor de la xarxa pública que té accés a la xarxa d'aplicacions. Un administrador de sistemes necessita accedir als servidors d'aplicacions a través del bastió.

A la **xarxa d'aplicació** hi trobem els següents tipus d'aplicacions:

- Aplicacions **consolidades** (php-c10d): Els servidors consolidats allotgen aplicacions PHP que es connecten a un MySQL amb un CMS (Wordpress o Drupal). Són les aplicacions més usades en la infraestructura.
- Aplicacions **docker** (app-docker): Les serveis docker solen estar en un servidor a part. Per la seva casuística concreta no s'ajusten a les tecnologies usades en els consolidats i per això estan desplegades en contenidors.
- Aplicacions **python** (app-py): Les aplicacions python són aplicacions fetes a mida, per exemple, les que pugui haver creat APSL. Usen Python com a llenguatge de programació juntament amb altres tecnologies i també s'allotgen en el seu propi servidor.

A la **xarxa privada** hi trobem les següents bases de dades:

- MySQL Aurora: Servidor que allotja les bases de dades de tipus MySQL. Cada aplicació consolidada té la seva pròpia base de dades en aquest servidor.
- PostgreSQL: Bases de dades per les aplicacions Python.

Les bases de dades de les aplicacions estan separades i cadascuna té el seu usuari per només tenir permisos en el seu àmbit.

A **xarxa d'administració** hi ha serveis diversos. Són aplicacions que serveixen per administrar altres aplicacions i són usades pels administradors de sistemes o els tècnics de la DTI. Estan separades a una xarxa apart per tenir major control i menor exposició.

Els serveis desplegats a la xarxa d'administració son:

- Gestor de configuracions SaltStack
- Gestor d'aplicacions Sygox
- Sistema de monitorització CheckMK
- Sistema de recollida de mètriques i visualització InfluxDB + Grafana
- Director de servidor de còpies de seguretat.

Quin recorregut segueix una petició?

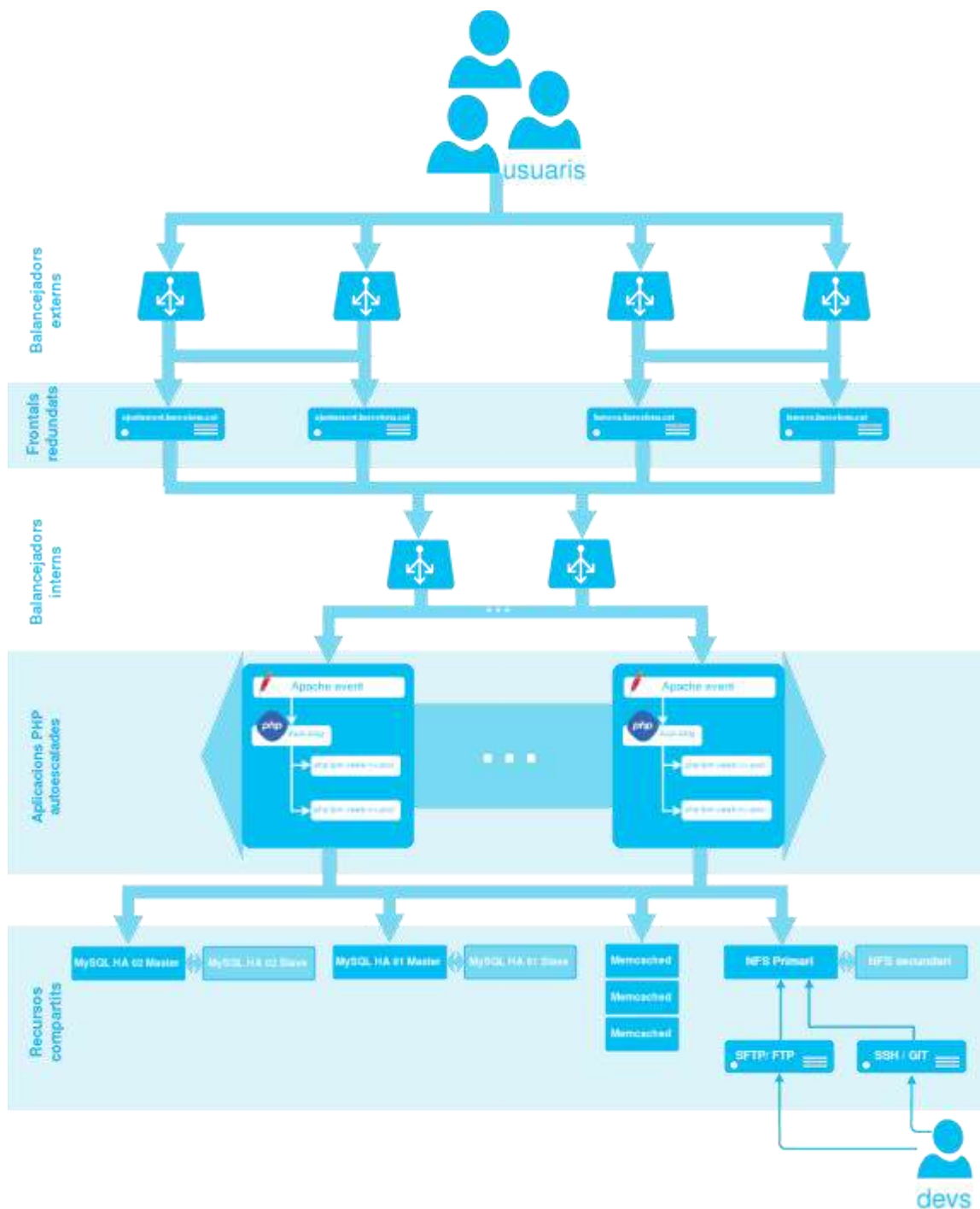
Troblem tres tipus d'usuaris de la infraestructura:



- **Usuari comú (HTTPS):** El seu interès és consultar una aplicació, per exemple <https://www.barcelona.cat/nadal>. Quan s'accedeix a la url es fa una petició a la CDN, aquesta consulta al frontal que, a l'hora, redirecciona la petició cap al servidor consolidat de tipus php-c10d-static-XX, on hi hagi l'aplicació *nadal*. Aquesta és una aplicació consulta la seva base de dades MySQL al clúster Aurora.
- **Tècnic de la DTI/Desenvolupador (desplegar codi):** L'interès d'un tècnic de la DTI o d'un desenvolupador és, generalment, accedir per fer un desplegament del codi de l'aplicació. Per fer-ho s'usa el protocol SSH amb l'eina anomenada SSHail. Es fa una petició al servidor de tipus sshail-01, a la xarxa pública, qui serà l'encarregat de crear una connexió nova cap a un servidor consolidat per tal de poder accedir al codi de l'aplicació. El SSHail és un programari de dos factors. El primer es una autenticació HTTPS que dona el host i port on connectar-se. La segona connexió es fa amb una contrasenya auto-generada o clau SSH que prèviament el desenvolupador ha definit. Una vegada completada la tasca, el túnel es tanca i la connexió deixa d'estar disponible.
- **Administrador de sistemes:** Un administrador de sistemes, en aquest cas d'APSL, té la necessitat d'administrar el servidor com un tot, no pas a nivell d'aplicació. Per això accedeix per SSH al servidor que fa de bastió, de tipus *bastion-01* que té permisos per obrir connexions cap als servidors de la xarxa d'aplicació i des d'aquí fa un altre SSH al servidor de destí en qüestió.

13.2.4. Arquitectura dels clústers d'aplicacions i de BBDD

En aquest apartat es detalla l'arquitectura dels servidors on corren els webs.



Es disposa de balancejadors de càrrega per tal de poder enviar les peticions a més d'un frontal o servidor d'aplicacions.

Es redunden els frontals principals i estan darrera d'un balancejador per poder-los escalar o posar en mode manteniment sense provocar un tall de servei.

Es disposa d'una arquitectura amb un conjunt de servidors d'aplicacions relativament grans on cada un dels servidors d'aplicacions pot servir un conjunt de webs.

Cada un dels servidors d'aplicacions està amb un nivell de càrrega alt responent peticions de totes les webs, aprofitant els recursos de la màquina. Quan es calen més recursos es fa un



escalat horitzontal posant altres servidors que continguin totes les webs per balancejar la càrrega.

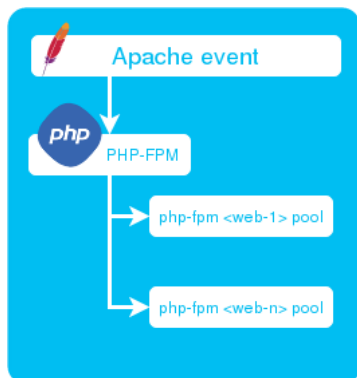
Per tal de poder tenir més d'un servidor d'aplicacions servint les webs son necessaris punts compartits on guardar dades. Es disposa de clústers de MySQL actiu/passiu. Si falla l'actiu el passiu passarà a oferir el servei.

Es disposa d'un clúster de Memcached per guardar les sessions del PHP.

13.2.5. Detall del servidor de aplicacions Apache + PHP-FPM

Els servidors d'aplicacions porten el codi de totes elles, per tant qualsevol servidor podrà servir totes les webs. Hi haurà un sol servidor Apache en mode MPM Event enviant les peticions diversos pool de processos PHP-FPM.

Cada web té un pool de processos PHP assignat amb un usuari de sistema únic per estar isolats entre ells a nivell de permisos.



Aquests pools només tenen processos actius si realment arriben peticions, en cas de no haver peticions els pools es van buidant de processos i **alliberen memòria** que pot ser emprada per els pools que si que tenen tràfic.

La memòria de tot el que són llibreries de PHP i els propis compiladors són compartits entre els processos fent que hi hagi més memòria disponible per el codi PHP de les aplicacions en si.

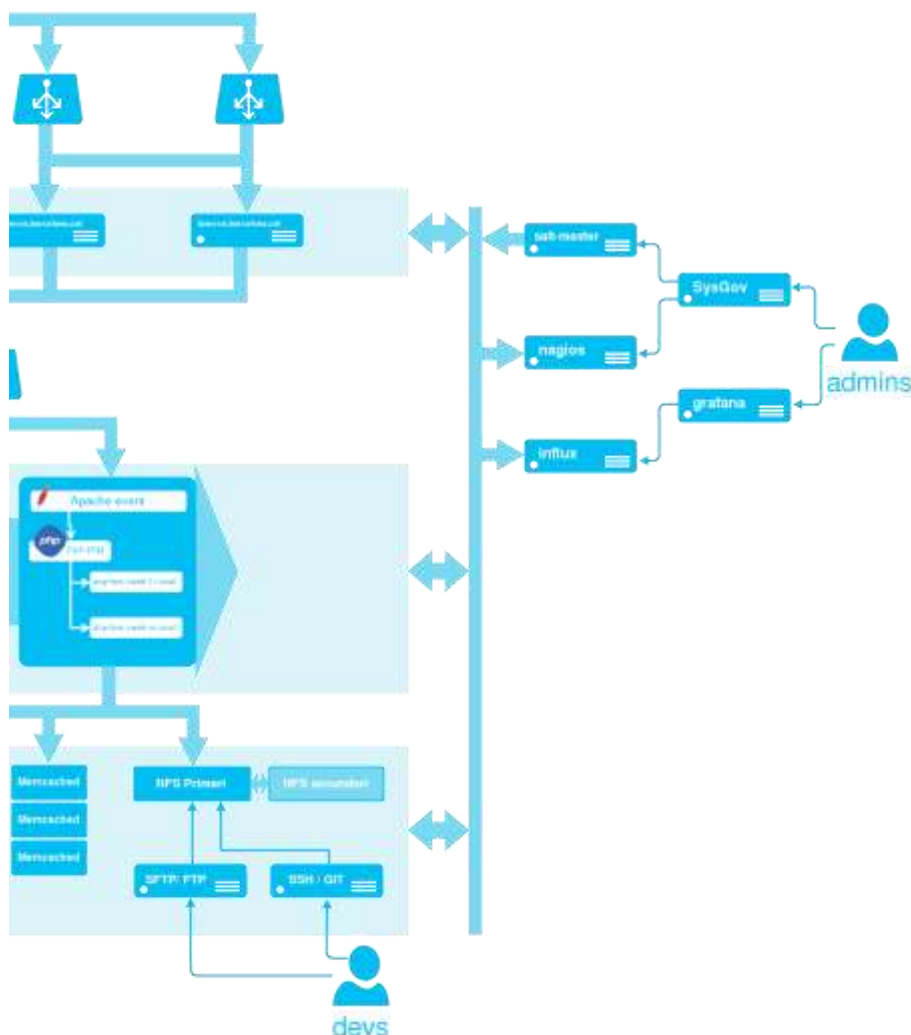
D'aquesta manera s'aconsegueix que la màquina estigui sempre ocupada aprofitant els recursos.

En cas que el servidor es vegi sobre-saturat i pugin els temps de resposta es desplegaran servidors idèntics en quan a característiques i configuració per tal de repartir la càrrega entre ells.

Per tal que els desenvolupadors puguin tenir accés hi haurà un altre servidor dedicat que muntarà el sistema d'emmagatzemament. Via aquest servidor, els desenvolupadors podran entrar i només veuran la seva carpeta. Podran tocar el que calgui dins el seu projecte, fent que es vegi reflectit de manera immediata al frontal.

13.2.6. Administració amb salt-stack

La gestió de configuracions es fa amb SaltStack.



Administració amb salt-stack: Els frontals

Donat que hi ha més d'un frontal, la configuració del mateix s'ha de fer de manera centralitzada. La solució aplicada és que SaltStack sigui l'encarregat de mantenir la còpia de la configuració i desplegar-la a tots als frontals un cop es faci un canvi.

D'aquesta manera no hi ha cap punt únic de fallada ja que SaltStack només és necessari alhora d'enviar un canvi o desplegar un nou servidor. Per altra banda mentre es serveixen peticions les màquines només depenen d'elles mateixes, cosa que no passaria si poséssim les configuracions en un emmagatzematge compartit.

Així doncs ja no es va al frontal principal a fer els canvis sinó que es faran les configuracions damunt SaltStack on hi haurà un repositori de codi.

A continuació es desplega la configuració en un dels frontals o un frontal de proves i serà provada. Aquí si es podria llançar una bateria de proves automatitzada per comprovar que els principals components funcionen.

Un cop validat es desplegaria la configuració a tots els frontals.

Amb aquest sistema no només tindrem alta disponibilitat als frontals sinó que es guarda històric de les configuracions aplicades i serà possible aplicar-ho i revertir-ho amb garanties.



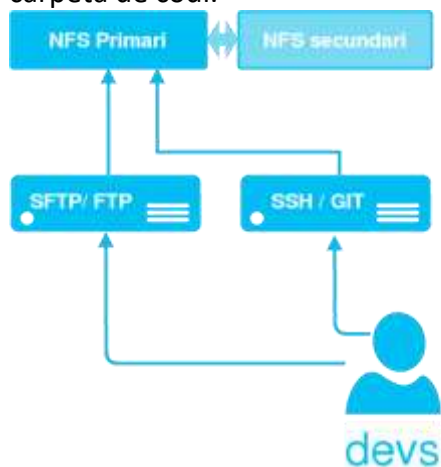
Administració amb salt-stack: Les aplicacions

Desplegar una nova aplicació web consisteix en generar la plantilla de configuració de SaltStack i aplicar-la als servidors.

Sygox consumirà una API donada per SaltStack on li passarà les dades de la web perquè aquest generi la plantilla i l'apliqui als servidors.

Així doncs l'accés de l'administrador de sistemes als frontals queda restringit a tasques de *debug* molt puntuals ja que no és necessari ni desitjable per fer les configuracions de les aplicacions.

Si un desenvolupador vol entrar a tocar el codi en viu de la seva aplicació hi haurà disponible una màquina que donarà accessos SSH i mantindrà al desenvolupador engabiat dins la seva carpeta de codi.



13.2.7. Característiques de seguretat/disponibilitat de la infraestructura (AWS)

En aquest apartat es mostren diferents punts en el que millora la seguretat o disponibilitat pel fet del canvi de proveïdor de núvol públic cap a AWS.

Arquitectura de xarxa

- Xarxes Privades Virtuals

Com s'ha descrit la xarxa està basada en Xarxes Privades Virtuals (VPC) i sub-xarxes on l'exposició a Internet varia en funció de la capa on s'està.

En la nova arquitectura la segmentació de xarxes permet reduir l'exposició dels serveis a Internet a nivell d'enrutat. Si un servei no té IP pública senzillament no és factible que s'hi arribi per accident des d'Internet oferint una molt bona capa de protecció.

Aquest avantatge és especialment bo per les bases de dades i eines de govern.

També és molt interessant per les aplicacions ja que només exposen els serveis, típicament HTTPS, a la cap de frontals, dins la xarxa pública, i aquests a l'usuari final.



D'aquesta manera l'únic punt d'entrada es un servei HTTPS cara als usuaris.

Al tenir tan reduïda la superfície d'exposició és més senzill registrar i filtrar les peticions amb un WAF com es mencionarà a punts següents.

- Ús de Security Groups

Els Security Groups són grups de regles de tallafocs que s'apliquen a nivell d'hipervisor de xarxa. Actualment els servidors disposen d'un tallafocs, l'UFW, basat amb iptables de GNU/Linux.

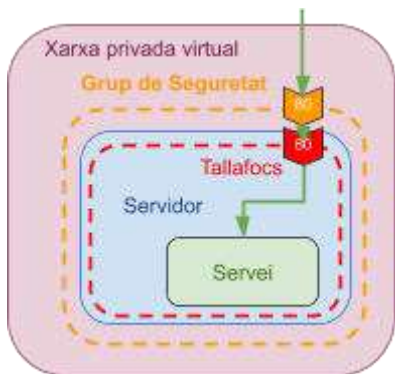
Amb els Security Groups a més del tallafocs del sistema operatiu hi ha una altre tallafocs que s'aplica independentment del que passi al sistema operatiu.

Suposem que un servidor ha estat atacat i l'atacant guanya permisos d'administrador. En un sistema tradicional podria modificar la configuració del tallafocs de la pròpia instància per sortir a internet, exposar ports etc.

Si el servidor disposa de Security Group encara que l'atacant modifiqui el tallafocs de la instància no pot manipular el tallafocs de l'hipervisor, per tant no serà capaç d'exposar nous ports ni modificar les regles de sortida.

Així doncs hi ha 3 capes de protecció a nivell de xarxa (de l'usuari al servidor):

- Sub-xarxa
- Grup de Seguretat
- Tallafocs del servidor



Les regles del tallafocs i del Security Group típicament són idèntiques així si algun dels dos falla, ja sigui per un atac o errada humana l'altre cobreix i es manté el servei protegit.

- Ús de múltiples zones de disponibilitat

A la infraestructura d'AWS es disposen de múltiples centres de dades amb baixa latència entre ells, on es poden compartir IPs. Els serveis en alta disponibilitat es despleguen amb



una instància a cada centre de dades i així s'és tolerant a fallada de centre de dades.

Serveis gestionats

- CDN (CloudFront)

Una Xarxa de Distribució de Continguts (CDN, en les seves sigles en anglès) és una xarxa d'ordinadors repartida arreu del territori i que té per objectiu disminuir la latència i incrementar la velocitat en que l'usuari rep les dades. Quan un client sol·licita dades al servidor obté una còpia des del punt més proper (edge), en comptes de fer-ho des de l'origen. En aquest sentit, si un client sol·licita per primer cop una informació que no es troba en el node de la xarxa més proper les dades seran descarregades des de l'origen al node en qüestió i després transmeses a l'usuari. Per tant els nodes edge a més fan de memòria cau (*cache*) i durant una quantitat de temps determinada aquesta informació romandrà en el node final i, passat aquest temps, serà invalidada i haurà de ser consultada de nou a l'origen.

Com a avantatge, a més, del servei de Cloudfront és que està tot gestionat amb [Terraform](#) amb els beneficis que això comporta.

- Bases de dades gestionades (Aurora RDS)

Actualment els serveis de bases de dades que emprem són dos:

- Servidors PostgreSQL
- Clusters MySQL gestionats amb Pacemaker / Corosync

Els **servidors PostgreSQL** són emprats per aplicacions Python/Django i eines de govern. Actualment són servidors sense alta disponibilitat ja que només disposen d'una instància.

A més, anteriorment eren servidors desplegats a la xarxa pública i exposats a internet filtrant les connexions per tallafocs per només acceptar-les del servidor d'aplicacions que corresponia.

El backup dels PostgreSQL era diari. Si es vol recuperar un backup anterior es perd un dia de dades.

En la **nova infraestructura els PostgreSQL** han sigut unificats en un clúster Aurora PostgreSQL d'AWS dins la xarxa privada sense exposició a internet. El clúster disposa d'alta disponibilitat en múltiples regions de disponibilitat. Els clústers Aurora tenen punt de restauració en el temps (PITR) i per tant es pot restaurar qualsevol punt dels últims 15 dies.

Amb la migració els servidors PostgreSQL estan en una xarxa més tancada minimitzant



el risc d'atac. A més s'ha incrementat la seva disponibilitat i es disposa de punt de restauració en el temps tenint major granularitat de recuperació en cas de desastre.

Els **clústers MySQL** actualment són 3 parells de servidors, així doncs tenim 3 clusters. Cada clúster està gestionat amb Pacemaker / Corosync per mantenir l'alta disponibilitat. n cas de fallada del principal el node secundari agafa el rol de principal. Per mantenir el sincronisme es generen logs binaris de l'últim dia, així doncs es disposa de punt de restauració en el temps de les últimes 24h, així com una còpia de seguretat diària.

A la **nova infraestructura els clústers MySQL** s'han fusionat i han donat lloc a 2 clusters nous. Un clúster per les aplicacions estratègiques i una altre per les aplicacions normals i en desenvolupament.

El clúster MySQL està en una xarxa privada sense exposició a internet només obert al servidor d'aplicacions.

Per defecte es tenen 15 dies de punt de restauració en el temps.

Cal mencionar que els clústers Aurora tant de MySQL com PostgreSQL es poden desplegar a múltiples zones de disponibilitat (fins a un màxim de 3). El nostre desplegament s'ha fet a dues zones de disponibilitat. Això significa que pot fallar un centre de dades sencer sense que s'interrompi el servei ja que el servidor desplegat a l'altre centre de dades agafa el rol primari.

- Certificats SSL

Els certificats wildcards s'estan deixant d'emprar, la qual cosa fa que el número de certificats gestionats sigui molt elevat. Actualment s'administren uns 300 dominis i es tendeix a que tots tinguin certificats únics.

Quan es compleixi això suposarà el manteniment i renovació de ~300 certificats, la qual cosa té un cost molt elevat, no només de certificat sinó sobretot de gestió i hores de feina de configuració i validació.

Amb AWS es pot millorar aquest flux ja que ofereixen un servei de certificats gestionats on es redueix significativament el cost en gestió i renovació del certificat.

El servei **ACM (Amazon Certificate Manager)**¹ permet tant importar certificats de tercers (per els que ja tinguem) com emetre certificats i renovar-los automàticament ja sigui emprant validació per correu electrònic o DNS.

Els certificats gestionats per ACM es poden desplegar als productes d'AWS com



balancejadors de càrrega o CDN.

ACM a més ofereix un panell integrat per veure quins certificats es tenen, quan caduquen i on estan desplegats però en cap cas deixa descarregar-los. Un cop introduït el certificat està completament protegit.

D'aquesta manera es passa a tenir una governança total del certificats, sabent on estan, perquè s'empren, controlant la caducitat i evitant que puguin ser compromesos de cap manera.

Es pot veure el detall del servei AWS a: <https://aws.amazon.com/certificate-manager/features>

- Monitorització

A dia d'avui la monitorització de la infraestructura es fa en base a dos serveis diferents.

Per una banda tenim el **checkmk**. Aquesta eina és usada pel sistema d'alertes per avisar els administradors de sistemes quan alguna cosa no està funcionant correctament. Amb ella es defineixen els llindars òptims de funcionament i quan algun paràmetre està fora de la normalitat salta l'alarma.

Per altra banda també tenim **Grafana**. Aquesta eina és usada per a la recollida de mètriques de la infraestructura i és especialment útil per visualitzar ràpidament l'estat dels sistemes.

Malgrat que són eines útils són gestionades completament pels administradors de sistemes d'APSL ja que **Digital Ocean no té un servei d'aquestes característiques**.

AWS compta amb el servei de Cloudwatch, eina administrada per AWS que té les mateixes funcionalitats, però ja de forma integrada a tots els serveis d'AWS. Val a dir que la migració a AWS no elimina ni checkmk ni Grafana, però sí que **dota d'una eina extra de monitorització que pot ser consultada també per tècnics autoritzats d'altres equips**.

A més a més, és un servei que estarà desplegat íntegrament amb [Terraform](#)

- Emmagatzematge estàtic en línia (S3)

Es fa us de S3 com emmagatzematge principalment amb 2 contextos:

- Emmagatzematge de llarga durada per redundància a les còpies de seguretat o arxivat
- Per emmagatzematge que se serveix públicament via web.



Buckets d'arxivat

En el primer cas s'empren buckets de S3 privats amb tipus d'emmagatzematge Glacier. Amb Glacier el cost per emmagatzemar grans quantitats de dades es redueix. A més per recuperar els fitxers s'ha d'enviar primer l'ordre de posar-ho disponible a S3 perquè després s'hi pugui accedir.

Els buckets d'arxivat mai son públics i s'empren credencials d'API específiques per accedir-hi.

En els buckets d'arxivat s'hi guarden còpies d'aplicacions que s'han donat de baixa a mode d'arxiu i còpies de seguretat que es volen tenir en més d'un proveïdor (el proveïdor habitual per les còpies redundants és Hetzner).

Buckets públics

Per altra banda també hi ha buckets on s'hi guarden recursos web estàtics que han de ser consultables per els usuaris.

En aquest bucket s'hi deixen fitxers no sensibles que son completament públics i que convé que estiguin altament disponibles o senzillament no es vol assumir el cost d'infraestructura en un servidor.

Típicament van emparellats amb una CDN per tal d'incrementar el rendiment amb que se serveixen als usuaris.

L'ús més típic seria guardar-hi imatges, fitxers Javascript o CSS per les webs.

S'empren claus d'API úniques per aplicació amb permisos mínims i granulars per pujar-hi els fitxers i es crea un bucket per cada aplicació evitant per evitar qualsevol tipus d'interferència o col·lisió entre aplicacions.

- **Emmagatzematge d'aplicacions en alta disponibilitat (NFS - EFS)**

Actualment l'emmagatzematge dinàmic de les aplicacions es troba amb discs SSD del proveïdor de cloud. Això significa que les dades només estan disponibles a un únic servidor. Si es volen implementar solucions d'alta disponibilitat es necessari desplegar serveis com NFS, GlusterFS, Ceph, DRBD, etc.

La complexitat de serveis de sistemes de sistemes de fitxers en xarxa que existien prèviament ha fet que no s'opti per aquestes solucions. Així doncs la major part de les aplicacions no estan en alta disponibilitat ja que no ho està l'emmagatzematge.

En la migració a AWS es passarà a emprar (un cop avaluat i ajustat el rendiment) el servei EFS (Elastic File System) que es un sistema de fitxers gestionat per AWS compatible amb NFS i disponible a múltiples zones de disponibilitat.



Això vol dir que es pot posar el codi i dades de les aplicacions en l'emmagatzematge compartit (EFS) i tenir múltiples servidors que hi escriuen i llegeixen. D'aquesta manera si cau un servidor l'aplicació segueix estant disponible.

El propi EFS està en alta disponibilitat i AWS garanteix una SLA de 99.99% amb compensacions econòmiques al següent cicle de facturació si no és compleix.

Com s'ha esmentat la disponibilitat del EFS no és només muntar un mateix sistema de fitxers entre diferents servidors sinó que aquests servidors poden estar a zones de disponibilitat (centres de dades) diferents i és següent garantit l'accés a les dades poden caure un centre de dades sencer i l'aplicació seguiria funcionant al centre de dades sa.

Mesures de contingència

- **Infraestructura com a codi com a pla de contingència**

El concepte de Infraestructura com a Codi (IaC) significa que el desplegament dels servidors està definit amb fitxers de text. D'aquesta manera hi ha un històric dels canvis i es poden comparar les diferències entre el que hi ha desplegat i el codi podent detectar canvis no desitjats o re-desplegar fàcilment una infraestructura.

A AWS es manté l'ús de SaltStack per la configuració del servidor però s'introdueix Terraform per el desplegament automatitzat de la infraestructura.

D'aquesta manera també es gestiona amb IaC la mida dels servidors, els Grups de Seguretat etc.

El fet de tenir amb IaC també el desplegament de servidors i serveis fa que regenerar la infraestructura en cas de desastre (o migració) sigui molt més senzill. Només s'ha de tenir un nou compte i aplicar les receptes primer d'infraestructura amb Terraform i després les de SaltStack reduint significativament el temps de recuperació en cas de desastre.

Eines de prevenció d'incidències de seguretat

- **WAF AWS Shield**

Actualment no es disposa de cap servei de tallafocs d'aplicació web (WAF). La intenció és un cop passat a AWS acollir-se al seu servei de WAF.

Per defecte la CDN (per on passarà el trànsit web) ja porta un nivell bàsic de WAF que inclou:



- Protecció contra atacs DDoS
- Anàlisi de trànsit basat en:
 - Firmes de transit (traffic signatures)
 - Algorismes de detecció d'anomalies
 - Anàlisi determinista de paquets
 - Mitigació per bloqueig i limitació d'ample de banda

A més del servei bàsic es contractarà el Shield Advanced que permet major personalització de regles i cobrir altres punts d'entrada a banda de la CDN.

AWS Shield Advanced permet:

- Personalització dels llindars per la detecció de l'atac
- Personalització de les regles de mitigació
- Integració amb l'estat de salut de les aplicacions
- Cobrir altres serveis a banda de la CDN com ara servidors concrets o balancejadors
- Línia de contacte amb l'equip de mitigació d'atacs d'AWS (DDoS Response Team, DRT)
- Vigilància proactiva de l'equip de DRT de la infraestructura
- Assegurança econòmica en cas d'atac dels recursos consumits en excés.
- Panells centralitzats de gestió de regles i visualització d'indicadors

Altres

- Ús de processos d'integració continua per minimitzar accés dels desenvolupadors als entorns productius.

Els accessos dels desenvolupadors per fer el desplegament son per SSH o sFTP emprant usuaris nominals, amb els mínims permisos per només poder desplegar el seu codi i restringides les comandes que poden emprar per només puguin fer el desplegament però no veure configuracions ni processos. A més hi ha capes de control addicionals com SSHail que s'han comentat a altres punts.

Aquests accessos fins ara eren imprescindibles per els tipus de CMS que s'estan desplegat i la metodologia dels desenvolupadors.

No obstant ja està implementat el projecte (a partir de Drupal 8) per emprar processos d'integració continua i desplegament continu (CI/CD).

Un dels objectius finals es que els desenvolupadors deixin de tenir accés als servidor



d'aplicacions productius i que el desplegament de codi es faci mitjançant accions associades al sistema de control de versions on a més queden traces de tots els canvis fets.

13.3. Reptes evolució infraestructura

Aquesta secció descriu les necessitats d'evolució de la infraestructura, amb l'objectiu **d'aportar informació detallada per les propostes de millora dels licitadors** que seran avaluades segons els criteris establerts a les clàusules administratives. Cal considerar tant la descripció detallada de la infraestructura existent en aquest apartat 13, com els requeriments específics de l'IMI (veure capítol "9 Requeriments específics", capítol "11: Condicions generals d'execució") i les tasques i responsabilitats indicades a l'abast (capítol "3: abast"). També si s'escau es pot sol·licitar la documentació ampliada que es posa a disposició sota demanda (veure "Annex 9).

Les propostes de millora han de ser capaces de compensar els costos d'implementació i manteniment associats. En moltes ocasions, es donarà preferència a solucions simples i fàcils de mantenir sobre aquelles que siguin excessivament complexes. Això significa que la simplicitat i la simplificació seran valorades positivament en les propostes presentades.

On s'escaigui, es pot incloure un anàlisi de cost/benefici a les alternatives de propostes per justificar les decisions preses. Aquest anàlisi pot ajudar a avaluar l'impacte financer de les propostes i a assegurar que les solucions proposades ofereixin valor afegit de manera efectiva.

13.3.1. Automatització

Recuperació automàtica dels webs

Es valoraran les propostes de contingències automàtiques fora d'horaris de suport per garantir l'alta disponibilitat dels webs, mitjançant la resolució automàtica de problemes puntuals de col·lapse, puntes de feina, i mal funcionament temporal.

Actualment els sistemes estan configurats amb uns paràmetres adequats adaptats a la necessitat de cada talla web per tal que puguin gestionar adequadament els recursos i quedin contingudes les incidències.

D'una banda, es configuren els CDN per absorbir la càrrega, i s'assegura una correcta configuració de les aplicacions en quant a que el ràtio de hits sigui òptim. En quant a les peticions dinàmiques que arribin a les aplicacions: s'ajusten els paràmetres del sistema com la mida de la cua, els temps d'espera, i el nombre màxim de processos concurrents. Això implica un seguiment precís de la càrrega màxima que pot absorbir un sistema, la quantitat de peticions per segon, i els temps de resposta de l'aplicació.



Per tant, és una arquitectura basada en una bona configuració i dimensionament, que es van ajustant segons estudi de la demanda, i que es complementa amb els ajustos obtinguts de l'experiència en incidències puntuals. Però actualment no hi ha previstos sistemes automàtics d'escalat dels nodes ni altres mecanismes que puguin reaccionar a una situació anòmala sense intervenció manual.

L'enfocament actual, doncs, es basa en la importància d'una bona configuració del sistema i un ajustament precís dels paràmetres per garantir un funcionament òptim sense necessitat d'intervenció manual freqüent.

Infraestructura com a codi (IaC)

Es valoraran les propostes d'automatitzacions de tasques d'instal·lació, configuració, manteniment, revisió, a fi de beneficiar-se de l'automatització dels canvis d'instal·lació i configuració d'infraestructures, del desplegament de webs, revisions de seguretat, i la traçabilitat dels canvis.

Com per exemple, propostes d'evolució de l'eina de govern (Sygox) per tal de donar autonomia als operadors (OT) o als desenvolupadors (programadors drupal), minimitzant així les tasques que s'han d'atendre.

Un altre exemple seria la millora continua a partir dels correctius que es donin: automatització de parts manuals, revisió procediments, preventius. Sempre que compensi el temps invertit en desenvolupament.

Actualment, l'aproximació a la infraestructura com a codi (IaC) forma part essencial de la estratègia per millorar i automatitzar la gestió de la infraestructura tecnològica. Aquesta estratègia inclou diversos aspectes clau:

- **Automatització de Tasques** d'instal·lació, configuració, manteniment, i revisió per beneficiar-se de l'automatització dels canvis d'instal·lació i configuració d'infraestructures, així com del desplegament de webs i revisions de seguretat. Aquest aspecte permetria reconstruir ràpidament parts de la infraestructura, a banda de conservar un registre de les configuracions i dels canvis.
- **Integració amb Sygox:** S'integra la gestió d'IaC en les eines de governança com Sygox, facilitant així l'autoprovisionament i permetent una gestió més autònoma de la infraestructura per part dels responsables de l'IMI.
- **Inventari i Gestió amb IaC:** Gestió del inventari dins les receptes, com per exemple redireccions de frontal, o configuracions de DNS.

Autoprovisionament

Es valoraran les propostes d'iniciatives encaminades a permetre l'autoprovisionament per part dels responsables de l'IMI, per tal de reduir hores d'operació de l'adjudicatari, i accelerar els temps de resposta de les peticions.

Sempre que es pugui, integrar la funcionalitat dins el "Sygox" donant una eina única d'interacció amb el sistema. Cal que donin una visió simplificada (per tal que l'operador



pugui dur a terme les peticions de manera senzilla), i siguin tolerants a errors humans (es puguin desfer els canvis).

Caldrà valorar en cada cas que compensi la seva creació (cost/benefici), alhora que el risc de alliberar informació crítica (potser caldrà mantenir un pas de verificació).

Actualment, l'autoaprovisionament es centra en permetre als responsables de l'IMI i als desenvolupadors tenir eines per realitzar operacions freqüents de manera autònoma, reduint les hores d'operació de l'adjudicatari i accelerant els temps de resposta. Aquest procés s'integra amb Sygox, proporcionant una eina única d'interacció amb el sistema. S'enfoca en oferir una visió simplificada i ser tolerants a errors humans, permetent desfer els canvis si cal.

Per analitzar quines tasques són susceptibles d'automatitzar, actualment es tenen en compte la freqüència de les peticions, la urgència la criticitat de les mateixes, la possibilitat de que s'incorporin errors o ineficiències al sistema en cas d'un mal ús. Amb aquesta informació es prioritza i es valora l'automatització. En alguns casos s'habilitaran controls o validacions en aquelles tasques crítiques que puguin suposar un problema per l'estabilitat o disponibilitat dels webs

Al manual de Sygox (veure "annex 9: informació ampliada que es posa a disposició") es pot veure el detall de tasques automatitzades i la funcionalitat que es proporciona actualment als desenvolupadors.

13.3.2. DevOps

Eines de control de desplegament

Es valoraran les propostes d'eines, desenvolupaments o automatitzacions que incrementin el control del codi desplegat pels desenvolupadors, i alhora permetin independitzar la localització del desplegament de la ubicació concreta on s'executa el codi del web per webs Drupal i Wordpress.

Exemple: evolucions del checklist, abstraccions del servidor on es treballa, monitorització de versions obsoletes, monitorització d'aspectes que afecten el rendiment un cop realitzada la sortida.

Un altre exemple: Proves d'Estrès i Rendiment Automatitzades: Integrar proves d'estrès i rendiment automatitzades al flux de treball de CI/CD per identificar possibles problemes de rendiment abans que afectin la producció.

Un altre exemple: Incorporació al circuit de revisió dels webs/aplicacions no inicialment en esquema devops.

Actualment es disposa d'un flux de desplegament automatitzat per versions drupal suportades i webs estàtiques, basats en el control de codi amb gitlab. Inclou un seguit de proves automàtiques (anomenada checklist) per comprovar la conformitat d'un web abans



de la seva publicació. Aquest procés no incorpora proves de rendiment. Tampoc incorpora la gestió de webs drupal de versions antigues, els webs wordpress, i algun framework php específic que no està suportat.

D'altra banda, també requereix l'execució manual de comandes al servidor productiu per instal·lar la versió (donat no està implementat encara la integració continua) degut a que això garanteix un major control, autonomia i validació del desenvolupador, fins que la maduresa de tot el sistema estigui garantida. En un futur es podria independitzar el desenvolupador dels entorns productius, però la quantitat de casuística diferent i la ràpida evolució de Drupal actualment no ho permet.

Eines de descobriment i gestió d'inventari de versions i d'estat de seguretat del web

Es valoraran les propostes de millores d'eines, desenvolupaments o automatitzacions que permetin millorar la gestió de l'inventari centralitzat de les característiques de cada web en quant a: producte instal·lat (drupal o wordpress), versions instal·lades (nivell d'aplicació d'actualitzacions de programari), versions dels mòduls instal·lats (tant de la comunitat com els específics de l'ajuntament), i altra informació rellevant per a la seva seguretat i manteniment (ex: usuaris, alertes, versions, configuració seguretat).

Inclou també la detecció i el reporting (i l'escalat als comitès si s'escau) de tots aquells aspectes de seguretat, rendiment, o risc destacables que s'obtingui a partir d'aquesta informació.

Actualment és un repte tenir actualitzada tota la plataforma, ja que implica mantenir uns sistemes que recopilin informació sobre les versions instal·lades de les aplicacions i les seves dependències. El cicle de vida de les versions de l'ecosistema Drupal s'ha accelerat notablement, amb la sortida de més versions i ritme d'obsolescència més ràpid de les antigues, i complicant la gestió de dependències (per exemple amb les versions de PHP, de MySQL, del drush, dels mòduls, etc.). Aquesta situació requereix una monitorització constant de les versions instal·lades i la planificació anticipada dels plans d'actualització massiu. També requereix la incorporació de noves versions de programari base (ex PHP) per tal que s'incorpori l'abans possible en noves aplicacions, per tal d'allargar d'entrada el seu temps de vigència.

Un dels reptes és plantejar i mantenir un full de ruta compartit entre desenvolupadors i l'equip de sistemes que mostri quines versions es poden utilitzar, i quines s'han de prioritzar durant la creació de webs noves (o les revisions de manteniment) per evitar feina de migracions futures.

13.3.3. Projectes

En aquest apartat l'Ajuntament valorarà les propostes concretes de cada licitador per desenvolupar solucions per unes determinades necessitats identificades. Si s'escau, i previ els ajustos que l'Ajuntament vulgui introduir, aquestes solucions proposades per el licitador podran ser executades dins el contracte com a recurrent.



Aplicatiu d'Arxiu històric de Webs

Es valoraran les propostes d'iniciatives encaminades a millorar l'emmagatzematge dels webs apagats (ja no visibles en producció) de forma que puguin ser activats sota demanda per a la seva consulta puntual i temporal, amb el mínim cost d'operativa.

Exemple: solucions per poder consultar puntualment webs dinàmics de manera interna, mitjançant la recuperació de backups, i no només les versions estatificades.

Exemple: ampliacions per tenir solucions d'estatificació permanent, i no només sota demanda, que permetés guardar periòdicament (per exemple mensualment) mostres del web per ser consultades internament sota demanda.

Actualment, es planteja el repte de com tenir disponibles per consulta interna totes aquelles webs que han acabat el seu període de publicació (per exemple web de nadal, web de sant Jordi, o altres del mateix tipus que cada any tenen imatge gràfica i contingut específic) o d'aquells webs que ja són obsolets (per un congrés, o d'algun alcalde concret), que ja no es vol tenir publicat però es volen tenir per ser consultables internament.

Cal tenir en compte que cada una d'aquestes aplicacions són de versions que pot ser que ja no estiguin disponibles a la plataforma, o que utilitzen serveis web interns o de tercers que poden estar despublicats.

Actualment es disposa de dues alternatives per consultar webs despublicats:

Primera alternativa: Estatificació dels webs

Mitjançant alguna eina d'estatificació, es transforma el web en html estàtic, que es pot tenir en un disc. La seva visualització no requerirà PHP ni BBDD.

- **Avantatges:**
 - La estatificació converteix els llocs web en arxius HTML estàtics, que es poden emmagatzemar fàcilment i consultar internament sense necessitat de tenir-los en línia.
 - L'ús d'eines d'estatificació pot automatitzar en certa mesura el procés, facilitant la conservació dels webs.
 - Al ser arxius HTML estàtics allotjats a S3, no consumeixen recursos a menys que siguin consultats.
 - Es poden usar diferents eines, ja siguin de codi lliure (com HTTrack) o bé de pagament, que només cal que estiguin instal·lades a l'ordinador de la persona que executa l'estatificació, i després no són requerides.
- **Desavantatges:**
 - Limitacions en la representació de llocs web dinàmics, com els que utilitzen components AJAX o els llocs web d'una sola pàgina (SPA).
 - Les funcionalitats amb parts dinàmiques dels llocs web, com els cercadors o els mapes, deixen de funcionar quan s'estatifiquen.
 - En ocasions no es pot estatificar totalment, degut a la gran profunditat o diferents maneres d'accedir a la informació, i cal definir una profunditat màxima.



- La captura es fa només sota demanda, i és un procés manual d'adaptació de les regles d'estatificació i validació del resultat. En ocasions calen ajustos manuals del web estatificat.

Segona alternativa: Restauració dels webs a través de backups

Es recuperen els webs en un entorn de desenvolupament, tant codi com base de dades, per tal de tenir-la 100% funcional.

- **Avantatges:**
 - La restauració dels webs a partir de backups permet recuperar els llocs web completament funcionals, incloent les parts dinàmiques i les interaccions amb serveis externs.
 - Aquesta opció proporciona una experiència més fidel al lloc web original, ja que es restaura totalment funcional.
- **Desavantatges:**
 - Requereix una tasca (hores de feina) de recuperació de backup, comprovació de bon funcionament, i adaptació del domini sobre el qual es serveix el web.
 - Pot ser més complicat i laboriós de configurar, especialment en casos de canvis de domini o dependències de serveis externs.
 - No hi ha autoprovisionament de llocs web antics, ja que cada restauració s'ha de fer de manera manual.
 - requereix que la tecnologia base (PHP, MySQL, etc.) estigui disponible.
 - Requereix que els serveis de tercers encara estiguin disponibles.

Actualment els requeriments no coberts de l'arxiu serien:

- tenir un sistema que permetés visualitzar webs LAMP més antics dels quals no es té les versions base.
- Disposar de sistemes proactius automatitzats d'estatificació (que no requerissin la petició d'estatificació ni ell treball manual) i que permetéssim tenir registre de canvis de webs importants d'evolució en el temps (per exemple tenien una solució similar a archive.org i /oPADICAT).
- Si s'escau, obrir una hemeroteca a la ciutadania per poder consultar webs despublicats

Aplicatiu de gestió de cues (puntual, sota demanda)

Es sol·licita la creació d'un sistema de cues que pugui ser configurat sota demanda (amb una determinada antelació, però que mentre no es faci servir no tingui cost o sigui molt baix) a qualsevol lloc web de l'ecosistema municipal. La finalitat principal d'aquest sistema seria gestionar de manera eficient les puntes de tràfic puntuals per pàgines concretes d'inscripció o tramitació, millorant així l'experiència dels usuaris i l'eficàcia de les plataformes digitals municipals.

Algunes de les característiques desitjades per a aquest sistema inclouen:



- **Gestió de Puntes:** Capacitat per controlar i limitar les càrregues de tràfic en moments de gran demanda, assegurant una experiència d'usuari fluida i sense interrupcions.
- **Priorització d'Accés:** Implementació d'un sistema que pugui prioritzar certes funcionalitats o serveis crítics en situacions de saturació del lloc web.
- **Monitoratge en Temps Real:** Un sistema que permeti supervisar la càrrega del servidor i la resposta del lloc web en temps real, facilitant la presa de decisions immediates.
- **Escalabilitat:** Capacitat per ajustar-se a l'augment de demanda sense afectar el rendiment global del lloc web.
- **Integració Fàcil:** Assegurar que el sistema de cues sigui fàcilment integrable amb qualsevol plataforma web existent dins de l'ecosistema municipal, minimitzant el temps i els recursos necessaris per a la implementació.
- **Seguretat:** Protegit contra la manipulació, ja sigui interna o externa.

Gestionar cues en el cas d'actes de ciutat amb moltes visites concurrents, com ara la reserva gratuïta d'entrades per actes de la Mercè, és un repte complex que requereix planificació, tecnologia adequada i una coordinació efectiva per garantir una experiència positiva per als participants. Els requeriments més rellevants serien:

1. **Altes càrregues de trànsit:** Amb molts ciutadans interessats en reservar entrades per a esdeveniments populars com els de la Mercè, les plataformes de reserva poden experimentar altes càrregues de trànsit simultani. Això pot provocar congestió del sistema i temps d'espera llargs per als usuaris, generant frustració i descontentament.
2. **Disponibilitat limitada de reserves:** Les entrades per a esdeveniments populars com la Mercè sovint s'esgoten ràpidament, i la demanda pot superar l'oferta disponible. Això pot crear una situació competitiva i augmentar la pressió per obtenir entrades, afegint encara més estrès a la gestió de cues.
3. **Equitat i transparència:** És important garantir que el procés de reserva sigui equitatiu i transparent per a tots els participants. Això implica establir regles clares i transparents per a la reserva d'entrades, així com garantir que tots els usuaris tinguin igualtat d'oportunitats per accedir a les entrades.
4. **Monitoratge i ajust continuat:** Supervisar el rendiment del sistema de reserva en temps real i fer ajustos segons sigui necessari per garantir una operació fluida i eficient.
5. **Seguretat i prevenció de frau:** Amb una alta demanda d'entrades per a esdeveniments populars, hi ha un risc de frau i abús del sistema de reserva. És essencial implementar mesures de seguretat efectives per prevenir el frau i garantir la integritat del procés de reserva.

Actualment l'IMI té contractat un servei extern de gestió de cues (de programari com a servei), fora de l'abast del present plec, que dona solució a moments puntuals de sobrecàrrega, especialment en tràmits o sistemes reserves que es donen en una hora determinada, amb el que es produeix molta concurrència.



Aplicatiu per mantenir al dia les versions globals, dur a terme actualitzacions massives, gestionar les polítiques de seguretat

Es sol·licita el desenvolupament d'aplicatius, procediments, automatitzacions que potenciïn la gestió i manteniment proactiva de les versions base, l'actualització massiva de webs obsolets i la implementació de polítiques de configuració i de seguretat.

Les característiques clau que busquem en aquesta plataforma inclouen:

- **Gestió de Versions Centralitzada:** Capacitat per monitorar i gestionar les versions de Drupal i WordPress de manera centralitzada, permetent una actualització fàcil i coordinada de totes les instàncies.
- **Actualització Massiva:** Funcionalitat per identificar i actualitzar massivament els llocs web desactualitzats, assegurant una ràpida i eficient implementació de les últimes versions i correccions de seguretat.
- **Validació automàtica:** garantir amb unes proves mínimes suficients que el web actualitzat segueix funcionant amb normalitat.
- **Polítiques de Configuració Automatitzades:** Establiment i aplicació de polítiques de configuració coherents per garantir la uniformitat i la conformitat amb els estàndards establerts en totes les instàncies.
- **Gestió de Seguretat Proactiva:** Implementació d'eines de seguretat integrades per identificar vulnerabilitats i aplicar pegats de seguretat de manera automàtica o amb intervenció mínima.
- **Alertes i Informes:** Sistema d'alertes en temps real i informes periòdics per informar sobre l'estat de les actualitzacions, la seguretat i la conformitat amb les polítiques establertes.

Ja s'ha plantejat en un anterior apartat la necessitat de disposar de manera clara i actualitzada del detall de totes les versions i dependències que s'usen en el sistema.

Tot i això en determinats moments es produeix la fi de suport de determinades versions, que pot afectar un gran nombre d'aplicacions. Dins l'àmbit del present contracte es pot encarregar que es duguin a terme actualitzacions de manera automatitzada d'un gran nombre d'aplicatius.

El repte de mantenir al dia les versions globals, dur a terme actualitzacions massives i gestionar les polítiques de seguretat s'enfronta amb diverses estratègies i protocols per assegurar la seguretat i l'actualització eficient dels sistemes. Aquestes inclouen:

- **Actualitzacions Massives:** El pla d'actuació contempla la realització d'actualitzacions massives, primer aplicant l'actualització de manera controlada en un servidor i, un cop comprovat l'efecte positiu, expandir-la a tota la infraestructura.
- **Gestió i Seguiment de Vulnerabilitats:** Es realitza un seguiment de les vulnerabilitats a través de bases de dades de CVE, permetent detectar possibles vulnerabilitats que puguin escapar al control del sistema de monitorització automàtic.



- **Suport als Desenvolupadors i Automatització de l'Actualització de CMS:** Es promou l'actualització automàtica dels CMS quan sigui possible, amb un enfocament especial en versions menors per assegurar la compatibilitat.
- **Inventari i Monitorització de Versions:** Es manté un llistat actualitzat de totes les versions del programari utilitzat, creuant aquesta informació amb bases de dades de vulnerabilitats per identificar possibles exposicions a CVEs.

Aquestes estratègies busquen equilibrar la necessitat de mantenir els sistemes segurs i actualitzats, minimitzant al mateix temps la intervenció humana i optimitzant els processos d'actualització per reduir els riscos de seguretat.

Suport intern per Intel·ligència Artificial

Es sol·licita el desenvolupament d'un aplicatiu automatitzat (basat en IA) per donar suport als desenvolupadors en diagnòstic de problemes freqüents, i en cerques ràpides de informació dins la documentació de la plataforma HOSTING LAMP.

Com a exemple, es proposen les següents funcionalitats, que s'han identificat com que serien profitoses:

- Aprofitar les tecnologies de Model de Llenguatge (LLM) per proporcionar primeres respostes útils als tiquets que es reben. Implementar un sistema eficient d'aprenentatge automàtic per millorar les respostes amb el temps.
- Indexació i Accés a la Documentació: Desenvolupar un mòdul que indexi de manera exhaustiva la documentació existent de la plataforma. Proporcionar accés a aquesta documentació mitjançant un sistema de xat per facilitar als desenvolupadors la cerca d'informació rellevant.
- Estar preparats per desplegar programaris en les webs que utilitzen o integren serveis de LLM, assegurant una integració suau i sense incidents.
- Suport a la Formació i Experiència dels Desenvolupadors: Introduir eines d'Intel·ligència Artificial per abordar dubtes relacionats amb la plataforma sense necessitat d'intervenció humana. Reduir les incidències causades per manca d'experiència o formació dels desenvolupadors, oferint respostes immediates a certs dubtes.

Aquest desenvolupament ha de seguir pràctiques de seguretat estandarditzades, assegurant la privacitat de la informació i complint amb les normatives vigents. El sistema ha de ser escalable per gestionar un creixent volum de tiquets i adaptar-se a les necessitats evolutives de la plataforma.

La intel·ligència artificial pot ser una aliada valuosa per als desenvolupadors a l'hora de trobar solucions als seus problemes en relació amb la infraestructura, de manera àgil sense esperar la resposta d'una consulta de suport de sistemes. Algunes maneres concretes en què la IA pot ajudar:

1. **Recerca avançada i filtrat de la documentació:** Un dels reptes més comuns per als desenvolupadors és trobar la informació rellevant dins de la vasta quantitat de documentació disponible. La intel·ligència artificial pot millorar la cerca i el filtrat de la



documentació, utilitzant tècniques com l'anàlisi semàntica per comprendre el contingut dels documents i presentar resultats més precisos.

2. **Assistència en la resolució de problemes:** Les eines d'assistència virtual basades en IA poden ajudar els desenvolupadors a resoldre problemes específics en temps real. Aquests assistents poden proporcionar orientació pas a pas, suggerir solucions basades en problemes similars resolts anteriorment o fins i tot executar comandes per provar solucions.
3. **Anàlisi de logs i telemetria:** L'anàlisi automatitzada de logs i dades de telemetria pot ajudar a detectar i diagnosticar problemes d'infraestructura de manera proactiva. La IA pot identificar patrons, anomalies i correlacions entre diferents factors que poden ser indicatius de problemes emergents.
4. **Traducció de documentació:** En entorns internacionals on els desenvolupadors parlen diferents idiomes, la traducció automàtica de la documentació pot facilitar l'accés a la informació rellevant per a tot l'equip de desenvolupament.
5. **Recomanació de millors pràctiques:** La IA pot analitzar els casos d'ús existents i les pràctiques recomanades per identificar i recomanar les millors solucions per a problemes específics d'infraestructura.

13.3.4. Robustesa

Evolució de clúster d'aplicacions

Es valoraran les propostes d'arquitectura evolucionada per allotjar els webs CMS i els Webs Estratègics, per exemple per potenciar:

- escalabilitat (possibilitat de créixer en més webs, més càrrega puntual d'aquests webs),
- isolació de recursos (un web donat no pot afectar els recursos d'un altre),
- alta disponibilitat (tolerància a puntes i a errors eventuais),
- desplegament controlat,
- estandardització del programari base i configuracions,
- facilitat monitorització del consum de recursos individual,
- accés als logs per part dels programadors,
- facilitat de replicació de la infraestructura,
- mobilitat de webs entre clústers
- protecció contra intrusions.

Tal com s'ha detallat a l'apartat 13.2 , les aplicacions s'executen en un clúster d'aplicacions. No s'ha realitzat la migració a containers donat que l'eficiència de recursos actuals és molt superior.

El dimensionament aproximat de recursos de cada talla de web actualment és:



TALLA	vCPU (*)	RAM (GB) (*)	espai disc SSD (GB) (*)	espai BBDD SSD (GB) (*)
Web CMS Estàndard	1/20	50 MB	2 Gb	0,5 Gb
Web CMS Estratègica	2/20	125 MB	4 Gb	1 Gb
Web CMS entorn desenvolupament	0,5/20	25 MB	2 Gb	0,5 Gb

Notes:

- L'Allotjament actual és AWS (Amazon Web Services, a la zona d'Irlanda)
- El càlcul del repartiment dels recursos mitjans s'ha tingut calculat en base al consum i la infraestructura actual:
 - Actualment conviuen unes 40 webs a cada clúster d'aplicacions consolidat. Les característiques d'aquest servidor: 2CPU , 4GB
 - Hi ha una mitjana de 200 BD per clúster (servidor 4CPU / 8GB).
 - Així doncs una web ocupa un 1/40 dels servidors d'aplicacions , i 1/200 del clúster de BBDD de mitjana.
 - Ara bé, cal tenir en compte que el web quan rep una petició consumeix molt més de 1/40 i 1/200 dels servidors, però a la pràctica mai hi ha totes les webs actives (dins del mateix segon) d'un clúster o servidor d'aplicacions.
 - De fet si el clúster té 8G de RAM i tenim 200BD no podem dir que cada web ocupa 40MB de RAM al clúster perquè no és cert. Puntualment n'empren molt més i amb un servidor de 40MB cap RAM (ni 128MB) cap de les webs funcionaria correctament.
 - Si es tractés de talles d'aplicacions individuals les xifres han de ser altes perquè si estiguessin soles serien necessàries ja que l'aplicació ho necessita
 - Per les aplicacions que es gestionen es calcula que el PHP consumeix uns 128M de RAM (màxim per defecte permès als settings actuals) i la BD uns 512MB de RAM.

Actualment, per tal de mantenir el cost a ratlla es donen a terme revisions periòdiques del consum de cada aplicació i es col·labora amb els desenvolupadors pertinents en cas de detectar una desviació del rendiment o abús de la càrrega d'un web determinat. Per webs normals no crítiques es considera millor una política de limitació del consum que no pas un es polítiques d'autoescalat que en cas de problemes podríem portar a costos molt alts. Es combina amb una revisió periòdica dels recursos assignats.

En quant al **clúster de base de dades**: Per tenir un servei equilibrat en cost/benefici, actualment s'utilitzen instàncies de servidors amb programari gestionat per Amazon amb les imatges d'aurora. Com a benefici es té com a servei tota la gestió de còpies de seguretat (amb punts de restauració un moment en el temps de manera fàcil) i l'aplicació de pegats del programari. S'utilitza una infraestructura actiu passiu per poder donar l'alta disponibilitat en cas de falla de la base dades.



Contingència

Es valoraran les propostes de contingència (en la nova infraestructura proposada que l'adjudicatari hagi escollit com a nova ubicació dels webs), en cas de falla greu en el datacenter, impossibilitat de connexió, o discontinuïtat dels serveis del proveïdor on s'allotjaran els webs. Ha d'inventariar possibles casos de desastre, i proposar possibles contingències amb el cost aproximat d'implementació (en hores) .

Les propostes de contingència en la nova infraestructura proposada se centren en l'anàlisi de possibles escenaris de desastre i la implementació de solucions per garantir la resiliència i la recuperació ràpida en cas d'incidències greus. Aquests escenaris inclouen pèrdua de dades d'una aplicació, fallada o pèrdua d'un servidor d'aplicacions, fallada o pèrdua dels servidors frontals, del sistema d'emmagatzematge, o d'un servidor del clúster de bases de dades, així com la fallada del proveïdor de cloud al complet.

Per afrontar aquests reptes, s'ha redissenyat tota la infraestructura per ser redundat i permetre l'autoescalat quan sigui possible, especialment en els servidors d'aplicacions. A més, s'emfatitza la implementació de la infraestructura com a codi (IaC), que permet que qualsevol element de la infraestructura pugui ser reproduït en pocs minuts. Això inclou tenir snapshots diaris dels servidors crítics, permetent una recuperació ràpida sense necessitat de reconstruir-los des de zero, sinó desplegant-los a partir d'un snapshot.

En cas de desastre total, com ara la fallada completa del proveïdor de cloud, s'ha contemplat un escenari on es migraria la infraestructura a un altre proveïdor, amb backups de la infraestructura redundats , emmagatzemats fora de AWS.

Contenidors i plataforma Kubernetes fins a 2 punts

Actualment els webs LAMP estan desplegats en clusters, i les aplicacions en contenidors en servidors virtuals amb docker compose.

Es valorarà l'estudi de viabilitat i aplicabilitat de desplegar els webs Drupal i Wordpress en forma de contenidors (Docker o similars) a la infraestructura del present projecte, concretant el mode de desplegament i el nombre d'imatges per web, la proposta d'eines i de canvis a la infraestructura actual, sistemes de monitorització , i destacant avantatges i inconvenients, impacte econòmic a la infraestructura i cost de serveis o llicències, dificultats i reptes d'aplicabilitat a l'entorn de l'Ajuntament.

Moure les aplicacions Drupal a contenidors pot oferir diversos beneficis en termes d'escalabilitat, gestió i implementació. No obstant això, també és important considerar els costos i els desafiaments associats a aquesta migració:

Beneficis

- **Flexibilitat i Escalabilitat:** Els contenidors permeten desplegar fàcilment les aplicacions Drupal en qualsevol entorn, facilitant l'escalabilitat vertical i horitzontal segons les necessitats del tràfic web.



- **Consistència en els Entorns:** Els contenidors proporcionen un entorn consistent per al desenvolupament, proves i producció, reduint els problemes de "funciona en el meu ordinador".
- **Desplegament Ràpid:** Amb els contenidors, els desplegaments i les actualitzacions poden ser més ràpids i menys propensos a errors, ja que cada contenidor opera de manera independent.
- **Optimització de Recursos:** La virtualització a nivell del sistema operatiu que ofereixen els contenidors permet una millor utilització dels recursos en comparació amb les màquines virtuals.
- **Aïllament de Dependències:** Cada aplicació Drupal pot tenir les seves pròpies dependències empaquetades dins del seu contenidor, evitant conflictes entre aplicacions.

Desafiaments i Costos

- **Complexitat de Gestió:** La gestió de contenidors pot ser més complexa que la gestió d'aplicacions en entorns tradicionals, especialment quan s'escalen a molts contenidors.
- **Seguretat:** La seguretat dels contenidors és crucial, ja que una mala configuració pot exposar el sistema a riscos de seguretat. És necessari implementar pràctiques de seguretat específiques per a contenidors.
- **Costos d'Infraestructura:** Encara que els contenidors poden optimitzar l'ús dels recursos, la infraestructura necessària (com ara orquestradors de contenidors) pot suposar costos addicionals.
- **Formació del Personal:** El teu equip pot necessitar formació addicional per gestionar eficaçment les aplicacions en contenidors, incloent l'orquestració i la seguretat.
- **Migració i Integració:** El procés de migració de les aplicacions existents a contenidors pot ser complex, especialment si les aplicacions no estaven dissenyades tenint en compte la inclusió en contenidors.
- **Avaluació de ús de implementacions propietàries:** Cal valorar també el benefici/cost d'ús de serveis de containers o de k8 com a servei, en front de configurar-ho sobre de servidors.

Còpies de seguretat (backups)

Es valoraran les propostes de millora o d'implementació d'eines i procediments de còpies de seguretat i recuperacions de dades, en el sentit que s'optimitza la freqüència de còpia, la rapidesa recuperació, la granularitat de la recuperació, l'espai total que el conjunt de còpies ocupen, asseguri la integritat de la còpia sense tall de servei dels webs (donat que els webs estan funcionant durant la còpia), no afectació al servei (no ralentitzi els webs), i el cost total de propietat.

Actualment s'utilitza Bareos, que ens permet fer una gestió eficient dels backups. Bareos és una solució integral de gestió de còpies de seguretat per a xarxes de sistemes informàtics, destacant-se per la seva arquitectura client/servidor que facilita la gestió de backups, restauracions i verificacions de dades. Aquest sistema ofereix funcionalitats avançades per a



la gestió eficient de l'emmagatzematge de dades, permetent la recuperació ràpida d'informació perduda o corrupta.

La monitorització dels backups i serveis de Bareos s'efectua a través de checks NSCA, amb els resultats enviats al servidor de monitorització checkmk, accessible a través d'una URL específica. Això permet un seguiment constant de l'estat dels backups per garantir la seva correcta execució i integritat.

Per a la recuperació de dades, Bareos disposa de l'eina bscan, que facilita la importació de dades des de volums de backup a una base de dades de Bareos, permetent posteriorment la restauració de les dades mitjançant un job des de la consola de Bareos. Això és crucial, especialment en escenaris de recuperació després d'un desastre, on pot haver hagut pèrdua significativa de dades i infraestructura.

L'estructura de backups actualment inclou una àmplia varietat de serveis i aplicacions, com servidors PHP consolidats, aplicacions internes, bases de dades RDS, i aplicacions Docker, entre altres. La política de retenció de les còpies de seguretat varia segons el tipus de backup, requerint procediments específics per a la seva gestió.

Finalment, la recuperació de servidors implica passos específics com la recuperació de servidors des de imatges de disc (snapshots), assignació d'IPs flotants, recuperació de dades o logs perduts, i l'actualització de configuracions de xarxa, assegurant així la continuïtat del servei i la preservació de la informació crítica.

13.3.5. Seguretat

Securització de la infraestructura

Es valoraran les propostes d'iniciatives, eines, procediments, configuracions encaminats a proveir de major seguretat a la infraestructura, en quant a protecció contra atacs maliciosos, ocultar informació sensible dels sistemes, detectar i analitzar comportaments sospitosos de visites, aplicació de millors pràctiques de protecció de sistemes, rastrejar traces en cerca d'atacs maliciosos, i filtres actius per al tràfic web. Les propostes han de cobrir les necessitats i requeriments detallats al plec tècnic.

Actualment, a banda dels serveis propis del cloud, en els frontals de les aplicacions s'ha implementat ModSecurity, que aplica un conjunt de regles per detectar (DetectionOnly) i bloquejar (On) peticions malicioses. Les regles desplegades són: OWASP, AntiDOS, Wordpress. Es pot canviar el mode a nivell de d'aplicació consolidada. També es poden desactivar regles a nivell d'aplicació. S'han implementat capçaleres de seguretat pròpies per Drupal i Wordpress, en concret: la Modificació de capçaleres amb Seckit, i la implementació de capçaleres X-XSS-Protection, CORS, Subresource Integrity, Content Security Policy, X-Frame-Options i X-Content-Type-Options.



Securització de webs LAMP

Es valoraran les propostes d'iniciatives, eines, procediments, configuracions encaminats a prevenir els atacs més freqüents contra els productes Drupal i Wordpress: detectar anticipadament configuracions febles als webs desplegats, fer seguiment de les vulnerabilitats greu obertes, aplicar mesures preventives als vectors d'atac més comuns, detectar ràpidament infeccions o intrusions en els webs.

Per exemple, es podria avaluar la integració d'eines d'anàlisi de seguretat estàtica i dinàmica en el cicle de desenvolupament per identificar i posar remei a vulnerabilitats de seguretat i/o males pràctiques de manera proactiva.

La verificació del codi dels aplicatius Drupal i WordPress des d'un punt de vista de seguretat implica diverses pràctiques i eines específiques. Es pot revisar varis aspectes tant que afectin a la seguretat i el rendiment, com poden ser:

- Validació i Sanejament d'Entrades: Assegurar-se que totes les entrades d'usuari són validades i sanejades per prevenir injeccions SQL, XSS, i altres vulnerabilitats.
- Autenticació i Gestió d'Accés: Verificar que les polítiques d'autenticació i gestió d'accés siguin robustes, incloent contrasenyes segures, autenticació de dos factors, i permisos mínims necessaris per a cada rol.
- Gestió d'Errors i Logging: Assegurar que la gestió d'errors no reveli informació sensible i que el sistema de logging capturi adequadament els esdeveniments rellevants sense exposar dades personals.
- Comunicacions Segures: Confirmar que totes les comunicacions de dades són realitzades a través de protocols segurs com HTTPS.
- crides externes desacoblades: assegurar que les crides https externes com per exemple a APIs s'estiguin protegint per timeout, o els errors de resposta per evitar el col·lapse de l'aplicació

Algunes eines i Automatització que es podrien usar:

- Anàlisi Estàtica de Codi: Utilitzar eines d'anàlisi estàtica de codi com PHPStan, Psalm per a PHP, o plugins específics de seguretat per Drupal i WordPress, per detectar problemes de seguretat potencials en el codi.
- Scanners de Vulnerabilitats: eines com OWASP ZAP o Nikto poden ajudar a identificar vulnerabilitats conegudes en aplicacions web.
- Revisió de Mòduls i Plugins: Verificar que tots els mòduls, temes, i plugins provinquin de fonts fiables i estiguin actualitzats. A més, revisar el codi d'aquests components per identificar pràctiques insegures.

Cal avaluar el benefici/cost de cada una, també tenint en compte que es tingui disponibilitat d'analitzar i processar els resultats, i la quantitat de falsos positius que es poden tenir que poden arribar a ser contraproductius.

Protocol d'aplicació d'actualitzacions massives crítiques

Es valoraran les propostes detallades de passos a seguir en cas de publicació de pegats crítics que solucionen vulnerabilitats importants en versions que estiguin desplegades a la



plataforma, en el sentit que prioritzin i facilitin l'aplicació dels pegats, el control de versions i de pegats aplicats. També es valoraran propostes que incentivin l'interès tant del adjudicatari d'aquest contracte com del programador responsable de cada web en mantenir actualitzats tots els webs.

Es pot donar el cas de que des de sistemes calgui dur a terme una actualització massiva d'aplicacions:

- davant de casos de incidències crítiques que cal aplicar a totes les aplicacions afectades,
- per economies d'escala que pot ser més eficient fer una actualització massiva ,
- si es dona el cas d'alt volum de aplicacions que queden obsoletes i que pot ser que algunes d'elles no tinguin en aquell moment equips de treball que els mantinguin
- en alguna transformació específica general urgent, com pot ser l'adaptació de barres corporatives, o el pas a webs segures (HTTPS).

Actualment, primer s'executen uns pilots, es valora fins a quin grau es pot automatitzar el procés, i es plantegen lots d'actualització semi automatitzats, amb una validació individual manual de cada web per donar aprovació final. Es tracta d'una operativa adaptada a cada proveïdor, amb eines específiques per cada procés.

Protocol de resposta a possible intrusió/infecció d'un web o sistema

Es valoraran les propostes detallades de passos a seguir en cas de detecció d'infecció o intromissió no autoritzada a qualsevol sistema , aplicatiu o web, en el sentit que prioritzi el seu seguiment i resolució, que prioritzi la comunicació amb el departament de seguretat de l'IMI, i que minimitza l'afectació del servei dels webs al ciutadà , la protecció de la imatge de l'Ajuntament, i la protecció de la reputació dels dominis i el posicionament SEO dels webs.

Actualment se segueixen les directrius de les clàusules de seguretat del present plec, que ja indica els passos mínims, però cada proveïdor pot indicar les eines, procediments i mesures que consideri necessari i que apliqui habitualment en les seves metodologies.

Govern de certificats digitals

Es valoraran les propostes d'eines, procediments, automatitzacions encaminades a governar gran volum de certificats diferents, en el sentit que millorin el control de la configuració de cada certificat, la validació automàtica que les configuracions tenen un grau adequat, l'auditoria que les proteccions del certificat són efectives, l'alerta amb temps suficient que algun caduca, automatització de renovacions de certificats gratuïts (per dominis de test), manteniment de la informació de quins dominis estan xifrats i quins no, seguiment de la configuració de xifrat de cada web.

Actualment es disposa d'una infraestructura que conté certificats de pagament (emesos i custodiats per l'IMI), com també d'altres emesos per Amazon (per dominis interns de



desenvolupament o de gestió), i un gran volum de certificats “let's encrypt” generats automàticament (per serveis de redirecció), en total més de mil.

Els certificats emesos per IMI, que són per els webs a ciutadania, requereixen un protocol de renovació manual via correu que no és gaire àgil, en el qual es proporciona el CSR, es completa un document de consentiment, i finalment cal instal·lar el certificat i validar-lo. Per tots aquests, cal anar revisant manualment quins caduquen, i un parell de mesos abans iniciar el tràmit.

Per tant es plantegen diferents reptes:

1. **Gran volum de certificats:** Amb més de mil certificats, mantenir-los actualitzats i gestionar-los eficientment ja és una tasca significativa per si sola. Cada certificat requereix supervisió, seguiment i renovació regular per garantir la seguretat i el compliment dels requisits legals.
2. **Renovació manual dels certificats de pagament:** El procés de renovació manual dels certificats de pagament, que implica la generació de CSR, la presentació de documents de consentiment i la validació del certificat, és lent i propens a errors. A més, aquest procés sovint requereix la coordinació amb diverses parts interessades i departaments, afegint encara més complexitat i temps al procés.
3. **Termes de renovació anticipada:** Els certificats de pagament sovint requereixen renovació anual amb un termini específic. Cal començar el procés de renovació amb prou antelació per garantir que els certificats es renovin a temps, evitant així interrupcions en els serveis i problemes de seguretat.
4. **Riscos de complir amb els requisits de conformitat:** La gestió manual de alguns certificats digitals de pagament pot comportar riscos de complir amb els requisits de conformitat, com el PCI DSS (Payment Card Industry Data Security Standard). Els processos manuals poden deixar l'organització vulnerable a infraccions de la seguretat o a sancions per no complir amb els estàndards de seguretat.
5. **Càrrega de treball i recursos requerits:** La gestió manual de certificats requereix temps, esforç i recursos humans. Això pot ser costós i ineficient, especialment en empreses amb grans volums de certificats.

13.3.6. Infraestructura

Infraestructura destí

Es valoraran les propostes de nova infraestructura on s'executarà el projecte, destacant les diferències i avaluant els avantatges de les mateixes respecte les característiques actuals. Cal detallar proveïdor/s d'infraestructura, quins serveis del proveïdor s'usaran, quines aplicacions es mantindrien o es consolidaran, quins nous subsistemes es crearan a part dels especificats (ex: clústers, memòria cau, elements de control de tràfic), i la calendarització aproximada de la posta en marxa de cadascun dels canvis, per indicar el moment del contracte en el que es vol abordar.



Cal aportar el raonament que conclou que la infraestructura proposada és superior a l'actual, i també un anàlisi mínim de cost/benefici.

Les propostes han de cobrir les necessitats i requeriments al plec tècnic.

Actualment els serveis es troben desplegats a AWS Irlanda, i l'IMI considera que és l'elecció adequada en aquest moment per aquest projecte. De totes maneres, el licitador pot considerar, segons el seu coneixement o la disponibilitat de datacenters propis, o d'acords comercials amb altres clouds amb similars serveis, que té una proposta més avantatjosa.

Optimització de costos

Es valoraran les propostes d'optimització de costos que es duguin a terme durant la transició del servei o els primers mesos del servei, que estiguin encaminats a reduir els costos totals de la infraestructura facturada a l'Ajuntament. Inclou les següents iniciatives:

- optimització de la gestió de costos: procediments per analitzar el consum actual i detectar punts d'optimització.
- neteja d'aplicacions, emmagatzematge i configuracions identificats com a poc òptims, obsolets o redundants
- optimització de les configuracions de CDN per augmentar el ratio de caché i reduir el trànsit, especialment de les aplicacions PHP, cap als backend i bases de dades, per tal de reduir el dimensionament de la infraestructura.
- pas a MySQL 8 per tenir un guany en eficiència que pugui reduir el cost del clúster de BBDD.
- altres iniciatives de disminució de costos fixes on es pugui observar un benefici esperat, com per exemple conversió d'aplicatius a serveis, ús de serverless, estendre CDN a més dominis. Implementar pràctiques de FinOps per optimitzar els costos al núvol, monitoritzant i ajustant els recursos segons la demanda i utilitzant eines com AWS Cost Explorer.

Els costos variables del cloud públic, combinats amb la complexitat de la infraestructura, poden conduir a diverses ineficiències i sobre costos si no són gestionats adequadament. Algunes de les raons per les quals això pot passar:

1. **Escalabilitat i flexibilitat:** Si bé la capacitat de escalabilitat del cloud públic és una avantatge, pot portar a un ús excessiu de recursos si no s'administra de manera eficient. Les instàncies o serveis que no s'utilitzen de manera òptima poden quedar en funcionament, generant costos innecessaris.
2. **Complexitat de l'entorn:** Amb múltiples serveis, regions i opcions de configuració disponibles en el cloud públic, la gestió de la infraestructura pot tornar-se complicada. Les configuracions inadequades o mal gestions poden conduir a un malbaratament de recursos i costos innecessaris.
3. **Manca de visibilitat detallada:** Sense una visibilitat detallada dels costos i l'ús dels recursos, és difícil identificar i gestionar eficaçment les ineficiències. Revisar la factura del cloud només a nivell superficial pot ocultar despeses ocultes o ineficiències en l'ús dels recursos.



Per a mitigar aquestes ineficiències i assegurar uns costos òptims, és essencial dur a terme una supervisió i gestió proactives. Això inclou:

1. **Revisió regular de la factura del cloud:** Analitzar detalladament la factura del cloud per comprendre com es distribueixen els costos i identificar possibles àrees de millora. Això pot incloure la identificació de serveis o instàncies subutilitzades o la revisió de costos associats amb els serveis addicionals.
2. **Monitoratge del rendiment dels serveis:** Supervisar el rendiment dels serveis i les instàncies per identificar possibles anomalies o tendències que indiquin un ús ineficient dels recursos. Això pot implicar l'ús de mètriques com la CPU, la memòria i el temps de resposta per identificar i abordar problemes de rendiment.
3. **Gestió de l'espai de emmagatzematge:** Revisar regularment l'espai de emmagatzematge utilitzat i eliminar dades o recursos innecessaris per optimitzar l'ús dels recursos i reduir els costos associats amb l'emmagatzematge.
4. **Seguiment de l'ús dels recursos per projecte o departament:** Mantenir un seguiment de l'ús dels recursos per projecte o departament per identificar quins equips o projectes estan consumint més recursos i assegurar una distribució eficient dels mateixos.



14. ANNEX 2. VOLUMETRIES I DADES

En el present annex es tracten les volumetries pròpies del present contracte a partir de les quals s'obté l'import de licitació. S'ha indicat per a cada un dels Servei-Aplicació que conformen l'abast del present contracte i cada un dels serveis inclosos plec (manteniment correctiu, manteniment recurrent, evolutius recurrents i serveis transversals de manteniment) l'esforç necessari per realitzar les tasques associades. I per l'aprovisionament de la infraestructura, s'indica el detall de les talles i serveis actualment necessaris, i que s'han usat per dimensionar el contracte.

14.1. Introducció

La volumetria de nombre de webs i servidors, es pot trobar al document de càlcul de cost del contracte: "Càlcul detallat import de contracte_AM_HOSTING_LAMP".

En resum: Actualment es manegen un total de prop de **1.050 desplegaments** de webs CMS (incloent productives i desenvolupament), a més de **55 servidors** dedicats (incloent els containers d'aplicacions de gestió o sistemes d'informació a ciutadà), **5 serveis de programari com a servei** i **1 servei SaaS** (web de la mercè). En aquest moment no hi ha cap llicència.

S'han realitzat un total de 500 passos a producció els darrers 4 anys (entre webs noves i actualitzades), a càrrec de més de 300 desenvolupadors de diverses empreses. Per aquest any 2024 el departament de comunicació està liderant 65 projectes de webs nous.

Se serveixen de l'ordre de 4 mil milions de hits anualment. El pic històric de visites es va donar durant les festes de la Mercè amb un total de 200 mil hits per minut.

A destacar també un creixement sostingut d'aproximadament 10% en el nombre de webs/serveis, i per tant també de tràfic, espai de disc, i configuracions associat a aquets nous webs.

En resum, es destaquen aquestes volumetries de servei:



Volumetria Servei HOSTLAMP



El detall de les URLs d'aquest inventari de webs, servidors dedicats, emmagatzematge, llicències i projectes SaaS, es proporciona en un document complementari de "inventari de webs i servidors", que està a disposició del licitador que el sol·liciti (veure annex 9).

14.2. Esforç

S'entén per esforç el volum d'incidències tipus (IT) que es produeixen en el servei de manteniment correctiu de forma habitual, de peticions tipus (PT) que es produeixen en el servei de manteniment recurrent i en el servei d'evolutius recurrents de forma habitual i per als serveis transversals de manteniment el volum de tasca tipus (TT) que es requereixen normalment.

Aquest volum d'incidències tipus (IT), peticions tipus (PT) i tasques tipus (TT) s'ha calculat a partir d'una línia base, que és el resultat obtingut d'un recull de la informació existent de contractes realitzats amb anterioritat, de similar complexitat i entorn tecnològic.

L'esforç dels serveis de manteniment **correctiu** es representa en incidències tipus (IT) i el del manteniment **recurrent** i **evolutiu recurrent** en peticions tipus (PT) de cada servei/aplicació (en els casos que no hi hagi aplicació però existeixi un servei d'aplicació, i l'esforç es calcula per aquest servei).

L'esforç dels **serveis transversals de manteniment** i evolutius identificats (aquest darrer no aplica per aquest contracte) es representa en tasques tipus (TT) per cada servei/aplicació (en els casos que no hi hagi aplicació però existeixi un servei d'aplicació, i l'esforç es calcula per el total del servei).



S'estima un esforç d'una hora per cada incidència, petició i tasca tipus.

En general , prenent com a mostra l'any 2025 complet, hi ha la següent previsió d'esforç d'hores necessàries:

servei	IT Manteniment correctiu	PT Manteniment recurrent	PT Evolutiu recurrent	TT Serveis Transversals de Manteniment	TOTAL
Estimació hores anuals 2025	1.920,00 hores	643,10 hores	2.498,75 hores	3.840,00 hores	8.901,85 hores
dedicació en persones (*)	1,00 FTE	0,33 FTE	1,30 FTE	2,00 FTE	4,63 FTE

En el document Excel adjunt "**Càlcul detallat import de contracte_AM HOSTLAMP, Càlcul pressupost**" es mostren les taules amb la volumetria d'hores estimades dels diferents exercicis. I a la pestanya **Perfils** es pot consultar la distribució de perfils per cada servei.

14.3. Servei d'aprovisionament d'infraestructura

A banda, per la infraestructura, es desglossa en el nombre d'elements de cada talla segons la volumetria actual

En el document Excel adjunt "**Càlcul detallat import de contracte_AM HOSTLAMP**, pestanya **Infraestructura-Talles**, es pot consultar la relació de talles desglossades, indicant els requeriments tècnics i també indicant el nombre de cada una segons l'inventari actual. Aquests valors són els que s'usaran (conjuntament amb els preus/perfil) per fer el càlcul del cost total de licitació (veure apartat 4.6.5 facturació del servei d'aprovisionament d'infraestructura).

El **Servei d'aprovisionament d'infraestructura** es divideix en 3 subserveis, que comptabilitzen de manera diferent el seu cost:

- **Infraestructura Webs CMS (PaaS)**: Infraestructura clúster per donar servei al principal volum de desplegaments web (prop de 1.050 en total). Es tracta de webs informatius, basats en gestors de continguts (CMS) Drupal i Wordpress. Per a la seva facturació, s'han classificat els webs en **talles**, segons els seus requeriments de servei. Inclou en el cost el suport tècnic a infraestructura, que no es podrà facturar a banda dins altres serveis del contracte.



- **Infraestructura Servidors Virtuals Dedicats (IaaS):** Infraestructura específica per un conjunt donat d'aplicacions que per la seva càrrega i/o requeriments específics tenen una arquitectura més complexa i una infraestructura dedicada. Inclou el suport tècnic a infraestructura, que no es podrà facturar a banda.
- **Programari com a servei (SaaS):** Programari com a servei, que cal subcontractar directament a una empresa determinada per requeriments tècnics. Inclou suport tècnic infraestructura i administració de sistemes, delegat en l'empresa subcontractada.

A continuació es detalla com es calcula el cost per cada subservei:

14.3.1. Infraestructura Webs CMS (PaaS)

- **Talles de Web CMS:** S'han classificat els webs CMS inclosos en el contracte en 3 talles principals, depenent dels seus requeriments de servei. A continuació es detalla cada un dels tipus:

Web CMS Estàndard: Web general, amb un nombre de de visites no molt alt, de l'ordre de 1.000 visites/mes . Habitualment no requereix molt espai de disc.

Web CMS Estratègica: Webs principals de l'Ajuntament, reben un gran nombre de visites, milers setmanals. Han de tenir alta disponibilitat, han de tenir una bona freqüència de realització de còpies de seguretat, i procediments de recuperació molt ràpids. Les incidències relacionades amb aquestes Webs han de ser tractades com a urgents. L'espai de disc requerit és molt relatiu al projecte, no és proporcional a les visites, però es presenten unes mides mitjanes

Web CMS entorn desenvolupament: Servidors per entorn de Proves, No requereix còpies de seguretat molt freqüents, tampoc ha estar disponible durant nits ni els caps de setmana. L'espai de disc requerit és molt relatiu, depèn del projecte en desenvolupament. Sovint es tracta de clons de l'entorn de producció, i per això ocupa igual.

Detall del dimensionament de cada talla (*dades octubre 2023*):

TALLA	vCPU (*)	RAM (GB) (*)	espai disc SSD (GB) (*)	espai BBDD SSD (GB) (*)	Nombre unitats
Web CMS Estàndard	1/20	50 MB	2 Gb	0,5 Gb	538
Web CMS Estratègica	2/20	125 MB	4 Gb	1 Gb	57
Web CMS entorn desenvolupament	0,5/20	25 MB	2 Gb	0,5 Gb	448
(*) En promig, veure detall càlculs de recursos. L'Allotjament actual és AWS					

Notes:

- L'Allotjament actual és AWS (Amazon Web Services, a la zona d'Irlanda)



- El càlcul del repartiment dels recursos mitjans s'ha tingut calculat en base al consum i la infraestructura actual.
 - Actualment conviuen unes 40 webs a cada clúster d'aplicacions consolidat. Les característiques d'aquest servidor: 2CPU , 4GB
 - Hi ha una mitjana de 200 BD per clúster (servidor 4CPU / 8GB).
 - Així doncs una web ocupa un 1/40 dels servidors d'aplicacions , i 1/200 del clúster de BBDD de mitjana.
 - Ara bé, cal tenir en compte que el web quan rep una petició consumeix molt més de 1/40 i 1/200 dels servidors, però a la pràctica mai hi ha totes les webs actives (dins del mateix segon) d'un clúster o servidor d'aplicacions.
 - De fet si el clúster té 8G de RAM i tenim 200BD no podem dir que cada web ocupa 40MB de RAM al clúster perquè no és cert. Puntualment n'empren molt més i amb un servidor de 40MB cap RAM (ni 128MB) cap de les webs funcionaria correctament.
 - Si es tractés de talles d'aplicacions individuals les xifres han de ser altes perquè si estiguessin soles serien necessàries ja que l'aplicació ho necessita
 - Per les aplicacions que es gestionen es calcula que el PHP consumeix uns 128M de RAM (màxim per defecte permès als settings actuals) i la BD uns 512MB de RAM.

14.3.2. Infraestructura Servidors Virtuals Dedicats (IaaS)

A part dels Webs CMS citats anteriorment, que comparteixen infraestructura en un clúster, es requereixen Servidors virtuals dedicats per tal d'allotjar aplicatius amb requeriments específics, que tenen una arquitectura pròpia més complexa i infraestructura dedicada.

- **Talla de 'Servidors virtuals dedicat'**: S'han classificat els servidors virtuals dedicats inclosos en el contracte en varies talles, depenent dels seu dimensionament. A continuació es detalla cada un dels tipus.

Detall del dimensionament de cada talla (*dades: octubre 2023*):

TALLA	vCPU	RAM (GB)	SSD (GB)	PROVEIDOR actual	Nombre unitats
t3a.micro	2	1	50	AWS	7
t3a.small	2	2	50	AWS	28
t3a.medium	2	4	50	AWS	11
t3a.large	2	8	50	AWS	7
t3a.xlarge	4	16	50	AWS	0
t3a.2xlarge	8	32	50	AWS	0,08
Servidor dedicat gran	6 CPU	64	64TB (32TB útils amb RAID)	Hetzner	2



Característiques dels complements d'emmagatzematge estès que s'afegeix a la talla (*dades octubre 2023*):

TALLA	TIPUS	PROVEIDOR	Nombre unitats
Volum (EBS) de propòsit general (gp3)	EBS gp3	AWS	8.664
Volum (EBS) de baix rendiment (st1)	EBS st1	AWS	1.725
Emmagatzematge compartit en alta disponibilitat	EFS	AWS	0
Snapshots de disc	Snapshot	Digital Ocean	304

14.3.3. Programari com a servei (SaaS)

Es tracta de programari com a servei (SaaS), que es subcontracta al proveïdor de infraestructura.

Es tracta de serveis complementaris que es paguen per consum, i que no encaixen dins una talla com les anteriorment presentades, i tenen gran variabilitat (segons necessitats de l'Ajuntament i les visites rebudes), i per tant el més adient és el pagament segons import consumit mensualment.

El detall dels serveis actuals necessaris, i que s'han usat per al càlcul del preu de licitació són:

Servei	Infraestructura
CDN Cloudfront	AWS
API-Gateway	AWS
S3, Glacier, Deep Archive (incloent peticions i operacions API)	AWS
NextCloud Hetzner	Hetzner (CCX)
Cookiebot	Cookiebot

Durant el contracte es pot donar un canvi d'aquests serveis segons necessitats, el licitador pactarà els canvis amb l'Ajuntament en els comitès de direcció.

14.4. Llicències i productes

Es tracta de serveis complementaris que es paguen per consum, i que no encaixen dins una talla com les anteriorment presentades, i tenen gran variabilitat (segons necessitats de l'ajuntament i les visites rebudes), i per tant el més adient és el pagament de la llicència segons import consumit mensualment.

Actualment no es tenen llicències i/o productes contractats, però pot donar-se el cas donant l'execució del contracte.



15. ANNEX 3: ADINET

En els casos que apliqui (a confirmar per el cap de projecte de l'Ajuntament segons el cas), el desenvolupament haurà de contemplar aquesta metodologia.

L'adjudicatari seguirà la metodologia ADINET), detallada en el present annex, o la metodologia de desenvolupament àgil d'aplicacions de l'IMI, anomenada Scrum@IMI (veure Annex 4). ADINET està basada en l'ús d'eines de gestió de requeriments, gestió de defectes i proves que proporcionarà l'IMI a l'adjudicatari. L'ús d'aquestes és obligatori per l'adjudicatari.

La metodologia ADINET es divideix en les següents fases: llançament, elaboració, construcció i transició, les quals es descriuen a continuació.

15.1. Fase de llançament

La fase de llançament té com a principals objectius redactar un pla de contracte i elaborar un pla de riscos, consensuat entre el cap de contracte de l'adjudicatari i el cap de contracte de l'IMI, i basats en l'oferta realitzada per l'adjudicatari.

El pla de riscos ha d'incloure la descripció detallada d'aquells riscos i problemes que sorgeixin i s'identifiquin al llarg del desenvolupament del contracte. El contingut mínim del que ha de disposar és: objectius del pla, identificació dels riscos principals, accions mitigadores i preventives, calendari d'execució del pla i mecanismes de seguiment i control del pla.

Ambdós plans hauran de ser aprovats per el comitè de direcció del contracte, i addicionalment es convocarà una reunió de llançament o Kick-Off del contracte.

15.2. Fase d'elaboració

La fase d'elaboració té com a objectius identificar tots els requisits funcionals i tècnics del sistema i definir l'arquitectura sobre la qual es construirà aquest.

En aquesta fase, serà obligatori per part de l'adjudicatari elaborar una maqueta que inclogui les funcionalitats definides per tal de que l'usuari les pugui validar.

Un cop finalitzada la fase, l'adjudicatari haurà de presentar els següents productes i documentació per validar i acceptar: document visió amb els requisits del sistema, document glossari amb les definicions dels termes que requereixin ser detallats, casos d'ús del sistema i workflow, document d'especificacions o requisits no funcionals del sistema, maqueta, document d'arquitectura del sistema i pla de proves.

El pla de proves ha de contenir com a mínim les següents proves tipus per tal d'assegurar el correcte funcionament del sistema:



Tipus de proves	Casos
Unitàries	4 casos de prova unitària per a cada cas d'ús crític/principal
Integració	1 cas de prova d'integració per a cada requeriment d'integració
Rendiment	1 cas de prova d'integració per a cada requeriment de rendiment
Qualitat de codi	1 cas de prova d'integració per a cada requeriment de qualitat de codi
Usabilitat	1 cas de prova d'integració per a cada requeriment d'usabilitat
Accessibilitat	1 cas de prova d'integració per a cada requeriment d'accessibilitat
Funcionals	1 cas de prova d'integració per a cada cas d'ús com a mínim. Cada escenari d'èxit ha de tenir associada, com a mínim, 1 prova, i cada escenari alternatiu, com a mínim, 1 prova
Acceptació d'usuari (UAT)	1 cas de prova per a cada requeriment funcional

La fase d'elaboració es considerarà finalitzada quant el responsable del contracte de l'IMI accepti tota la relació de productes i documentació detallada anteriorment. Aquesta acceptació de documentació es portarà a terme al comitè de direcció.

15.3. Fase de construcció

La fase de construcció té com a objectiu la construcció del sistema en base als requeriments definits en fases anteriors.

Durant aquesta fase, es realitzarà un desenvolupament iteratiu, la duració de les quals serà entre 4 i 6 setmanes. Durant aquesta fase, s'haurà d'elaborar el document de disseny tècnic que també inclou el disseny de la base de dades.



L'objectiu d'aquesta fase és la construcció del sistema. Durant aquesta fase es realitzarà un desenvolupament iteratiu. Les duracions de les iteracions seran entre 4 i 6 setmanes.

Durant aquesta fase s'haurà d'elaborar el document de disseny tècnic que inclou el disseny de base de dades. Aquesta documentació ha d'incloure el lliurament de diagrames en fitxer (format estàndard importable des d'eines de modelatge).

Amb cada iteració s'actualitzarà el Pla de Proves en l'eina corresponent, tot incloent la definició dels casos de prova corresponents a les funcionalitats afegides. Es realitzarà el registre en aquesta eina del Resultat de l'Execució juntament amb l'enregistrament dels resultats obtinguts. Com a prova d'aquest enregistrament es pot utilitzar:

- Fitxer de resultats generat per l'eina d'execució de proves.
- Fitxer log de l'aplicació.
- Captura de finestres amb el resultat de les proves.

Aquests resultats es presentaran després de cada iteració al Cap responsable del contracte de l'IMI per a la seva avaluació i validació. Aquesta validació serà necessària per poder donar per tancada cada iteració i poder començar l'execució de la següent.

Abans de passar a la fase de Transició, per tant com a mínim a l'última iteració prevista del producte, caldrà que el Cap responsable del contracte de l'IMI validi el sistema construït amb la verificació dels resultats obtinguts en l'execució de totes les proves previstes al Pla de Proves.

Abans de tancar cada iteració es presentarà la documentació tècnica de cada iteració:

- Document de Disseny Tècnic

A la finalització de cada iteració, si l'IMI ho considera necessari, es podrà realitzar una validació del sistema construït per part de l'usuari.

15.4. Fase de Transició

L'objectiu d'aquesta fase és la finalització del contracte. Prèviament al seu tancament i dins d'aquesta darrera fase, es realitzaran les següents tasques:

- Validació de tot el sistema per part de l'usuari.
- Execució del Pla de Gestió del Canvi segons el Pla de Gestió del Canvi previst i aprovat a la fase anterior:
 - Comunicació del calendari de desplegament del sistema.
 - Formació del personal (tant usuaris com tècnics).
 - Desplegament a Producció. L'Ajuntament podrà participar en totes les activitats de posada en producció del sistema construït.
 - Traspàs a l'equip responsable del seu manteniment.
- Lliurament de la documentació del sistema:
 - Descripció funcional.
 - Descripció tècnica.



- Manual d'usuari.
- Manual tècnic o d'administració.
- Full d'escalats: l'adjudicatari és responsable d'elaborar i lliurar a l'IMI el Full d'escalats de l'aplicació desenvolupada. Aquest full s'haurà d'elaborar segons el model de plantilla utilitzat per l'IMI i d'acord amb les responsabilitats dels diferents equips i entorns tècnics existents a l'IMI. Aquest full ha de servir perquè el personal del SAU de l'IMI pugui escalar correctament les incidències relacionades amb l'aplicació objecte del contracte al tercer nivell del SAU.

El tancament d'aquesta fase de Transició està condicionada pel fet que el Cap responsable del contracte de l'IMI rebí i accepti formalment la relació de lliuraments inclosos a l'abast del contracte. L'acceptació formal del contracte es farà en reunió del Comitè de Direcció del contracte. El fet de no assolir els objectius d'aquesta fase de Tancament, suposarà la parada del contracte.

15.5. Plataforma VALID@

VALID@ és una iniciativa que persegueix instrumentar la gestió de la qualitat dels contractes de desenvolupament programari a l'IMI. Està composta per una sèrie d'eines que permeten a l'IMI guardar registre i establir mecanismes de control sobre dos àmbits bé diferenciats:

- Compliment d'ADINET des d'un punt de vista procedimental: Verificació del compliment dels checkpoints vinculat a cada iniciativa de desenvolupament bé sigui nou desenvolupament, evolutiu o solució d'incidències.
- Emplenament del pla de proves previstes en ADINET (funcionals i no funcionals): Registre de requisits i proves associades així com execucions vinculades a aquestes.

Valid@ se sustenta, a la data de publicació del plec, en la següent plataforma tecnològica que serà d'obligat compliment per als proveïdors que resultin adjudicatari:

Aspecte	Eina	Ús
Control de Checkpoints	TestLink	Registre de Checkpoints d'ADINET
Requeriments	TestLink	Registre de requeriments
Cas de proves	TestLink	Registre de cas de proves
Execució de proves	TestLink	Registre d'execucions de proves
Defects (entorns no	Bugzilla	Gestió de defectes en els



productius)		entorns no productius
Qualitat de codi font	PMF, Checkstyle i Findbugs	Anàlisi estàtica de qualitat de codi font
Usabilitat i accessibilitat	Checkstyle usabilitat i TAW	Anàlisi estàtica d'usabilitat i accessibilitat de pàgines web
Rendiment	JMETER	Proves de rendiment
Automatització	SELENIUM	Automatització de proves

L'IMI es reserva es reserva el dret de modificar aquesta plataforma avisant d'això als diferents proveïdors amb suficient antelació.



16. ANNEX 4 : METODOLOGIA AGILE SCRUM@IMI (METODOLOGIA ÀGIL PER A PROJECTES IMI)

En els casos que apliqui (a confirmar per el cap de projecte de l'ajuntament segons el cas), el desenvolupament haurà de contemplar aquesta metodologia.

La metodologia de desenvolupament àgil d'aplicacions de l'IMI, anomenada **Scrum@IMI**, està basada en el marc de treball Scrum i pràctiques d'enginyeria provinents d'altres models com Extreme Programming o DevOps.

Aquesta metodologia, disponible per a l'empresa adjudicatària, se suporta sota l'ús d'una plataforma ALM (Application Lifecycle Managment) amb eines de:

- Planificació del desenvolupament (releases, sprints, paquets de treball, defectes, etc.)
- Repositoris de documentació, codi i binaris
- Gestió de requisits i proves
- Automatització de les proves unitàries i funcionals
- Integració continua i Desplegament continu
- Control de la qualitat del codi, entre d'altres

El seu ús és obligatori per part de l'adjudicatari sense que suposi un cost addicional en llicències per al mateix.

Tota la documentació que es generi internament al desenvolupament haurà de gestionar-se amb les eines que es determinin a l'inici del projecte, preferentment en format wiki.

Les principals característiques d'aquesta metodologia es comenten segons el seu cicle de vida al següent enllaç:

https://ajuntament.barcelona.cat/imi/sites/default/files/marc_de_treball_scrumimi_per_proveidors.pdf

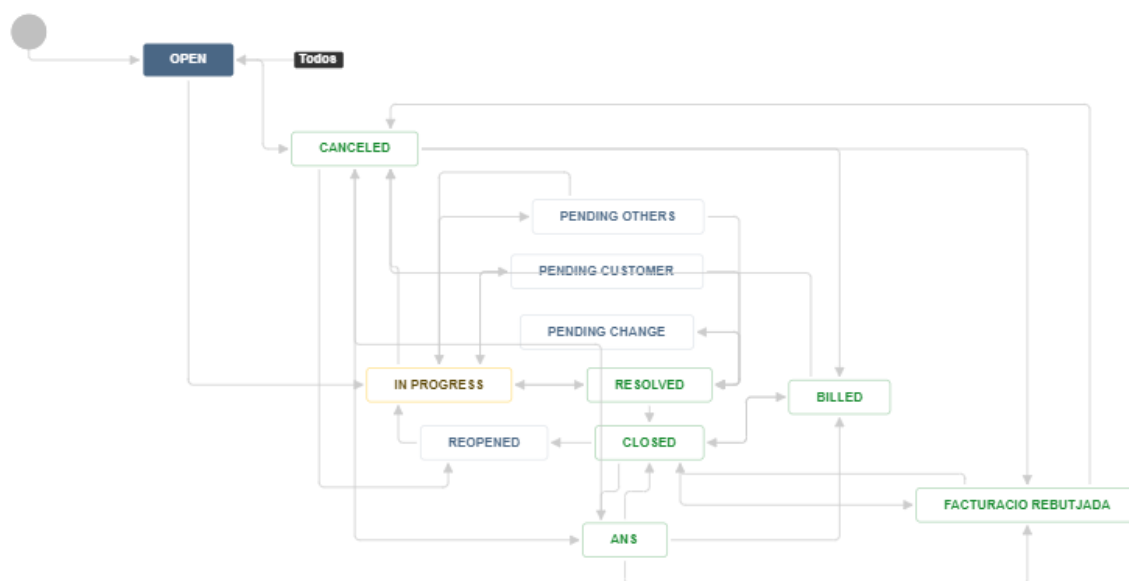


17. ANNEX 5 : FLUXOS A L'EINA DE TICKETING

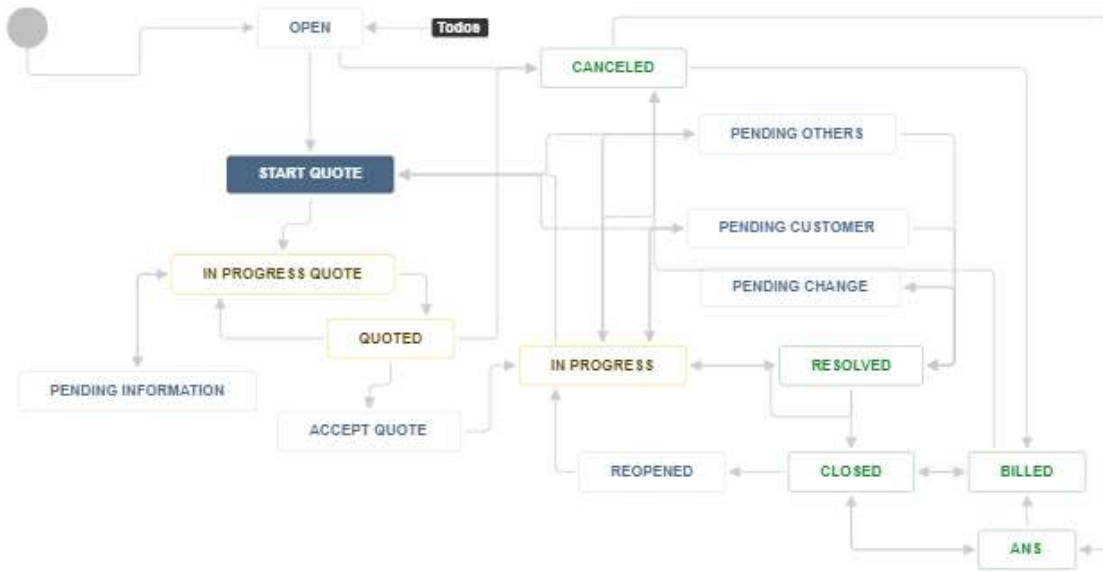
A continuació es detallen a mode il·lustratiu els fluxos, actuals en el moment de licitar el contracte, de tramitació dels manteniments a l'eina de ticketing.

Aquests fluxos poden variar durant l'execució del contracte, en aquest cas l'IMI comunicarà a l'adjudicatari els canvis en els fluxos.

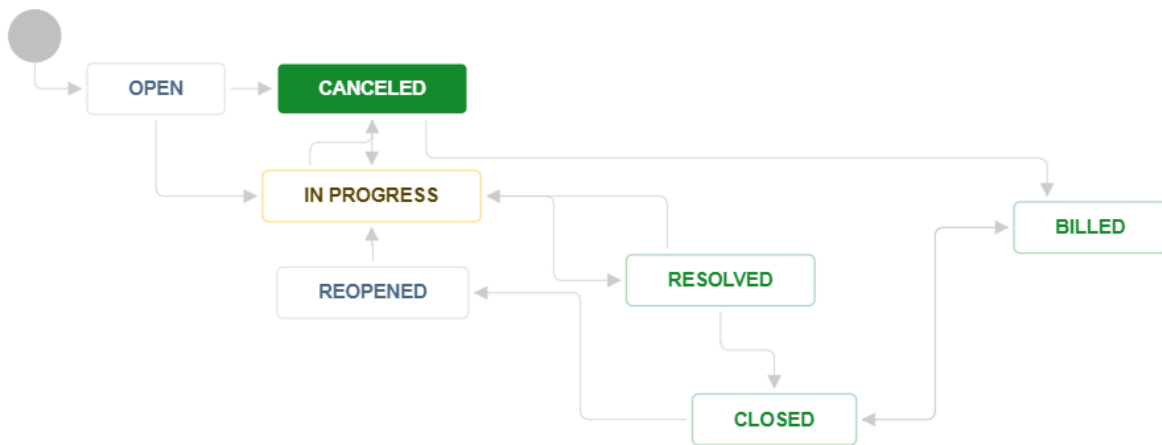
17.1. Manteniment correctiu



17.2. Manteniment recurrent, evolutius recurrents i evolutius identificats



17.3. Serveis Transversals de Manteniment





18. ANNEX 6: NORMATIVA DE DESENVOLUPAMENT. DESENVOLUPAMENT A MIDA AL CLOUD PRIVAT DE L'IMI (VERSIÓ 2020)

En els casos que apliqui (a confirmar per el cap de projecte de l'ajuntament segons el cas), el desenvolupament haurà de contemplar aquesta normativa.

18.1. Llenguatges de programació i Frameworks permesos

Els llenguatges "base" per programar les aplicacions a mida a l'Ajuntament de Barcelona:

- Backends:
 - Java
 - Python
 - R (Per casos concrets i especials com CityOS)
- Interfície Web (Single Page Applications)
 - Angular (TypeScript)
- Aplicacions al mòbil
 - Android
 - Kotlin
 - IOS
 - Swift

Comentaris:

- Quan el llenguatge escollit sigui Java l'IMI disposa d'un framework propi anomenat OpenFrameIMI i que, actualment, es troba en la versió 4. Aquest framework és d'**obligatòria utilització** per al desenvolupament d'aplicacions Java a **WebSphere**. Cal destacar que el framework openFrameIMI fixa l'arquitectura i els serveis per les capes de Negoci, integració i persistència.
- Quan el llenguatge escollit sigui Python, el framework ha de ser Django/Python i seguir les directrius de desenvolupament descrites a l'Annex 7.
- L'IMI **no fixa cap framework per a la capa de presentació**, però aposten per front-ends (SPAs Single Page Applications) implementats en Angular (en la seva última versió estable).

18.2. Entorns de desplegament:

Actualment, dins del cloud privat de l'IMI, tenim els diferents entorns de desplegaments possibles:

- Desenvolupament a mida:
 - Kubernetes, entorn de contenidors (Per defecte)
 - OpenShift 4.10
 - WebSphere Application Platform
 - J2EE: IBM HTTP Server for WebSphere Application Server 8.5.5 sobre SUSE Linux Enterprise Server 11
- Productes:



- Kubernetes, entorn de contenidors (Per defecte)
 - OpenShift 4.10
- Màquines virtuals
 - VMware vSphere 5.5

18.2.1. Tecnologies de desenvolupament

La plataforma d'orquestració de contenidors **al cloud privat de l'IMI** es basa en **kubernetes**. Aquesta plataforma permet el desplegament, a priori, de qualsevol llenguatge de programació i/o producte que es pugui dockeritzar. No obstant, l'IMI limita les diferents tecnologies en les que es poden implementar les seves aplicacions.

Actualment l'IMI permet les següents tecnologies i frameworks:

- Capa de serveis i/o de negoci (sempre parlem de versions estables)
 - Java:
 - Fwk 4 (Obligatori per les aplicacions desplegades a WAS)
 - Basada en java 8v192 i Tomcat 8.5.34
 - Framework de desenvolupament propi basat en Spring 2.5
 - Spring Boot
 - v. 2.6.4 o superior
 - Quarkus
 - v. 2.7 o superior
 - Python
 - Django
 - v. 4 o superior
- Capa de presentació
 - Framework SPA en **Angular**
 - v. 13 o superior
 - Framework SPA IMI (discontinuat):
 - Name: nginx-alpine-1.15.5-fwkspa
 - Basada en Angular 5
- Capa d'emmagatzemament de dades
 - Oracle 11g sobre SUSE
 - Servidor corporatiu
 - no en contenidors
 - La BD està fora de la plataforma kubernetes
 - És una instància Corporativa, 1 únic servidor de BD per n projectes
 - L'IMI gestiona aquesta infraestructura

A més d'aquestes tecnologies, i/o llenguatges de programació, l'IMI port permetre la utilització de d'altres productes com BD Redis, sistemes ELK, mongoDB destinades a accelerar, cobrir o millorar alguna funcionalitat concreta del producte resultant. No obstant, caldrà justificar clarament el perquè de la seva utilització i aquesta haurà de ser



aprovada pel departament de producció, el departament de seguretat i el departament d'arquitectura de l'IMI.

18.3. Directius a seguir en el desenvolupament i l'arquitectura

Es tracta de directrius independents de l'entorn de desplegament

18.3.1. Preparada per a ser Desplegada en Cloud

- El desenvolupament del sistema caldrà estar orientat a serveis. Tot el negoci de l'aplicació ha d'exposar-se mitjançant una o més API(s) de serveis.
 - Aïllar els serveis que l'aplicació necessita per a funcionar i implementar-ho com a una API independent, permetrà a aquest tenir la capacitat d'adaptar-se i escalar segons la càrrega o peticions que rebí, sense afectar a la resta de l'aplicació. A la mateixa vegada aquest disseny permet monitorar i gestionar amb més precisió els diferents components de software.
- La construcció de l'aplicació haurà de seguir els [12 Factors App](#):
 - I. Codi base (codebase) Un codi base sobre el qual fer el control de versions i múltiples desplegaments
 - II. dependències Declarar i aïllar explícitament les dependències
 - III. Configuracions Guardar la configuració en l'entorn
 - IV. Backing services Tractar als "backing services" com a recursos connectables
 - V. Construir, desplegar, executar Separar completament l'etapa de construcció de l'etapa d'execució
 - VI. processos Executar l'aplicació com un o més processos sense estat
 - VII. Assignació de ports Publicar serveis mitjançant assignació de ports
 - VIII. Concurrència Escalar mitjançant el model de processos
 - IX. "Desechabilidad" Fer el sistema més robust intentant aconseguir inicis ràpids i acabaments segurs
 - X. Paritat en desenvolupament i producció Manténir desenvolupament, preproducció i producció tan semblants com sigui possible
 - XI. historials Tractar els historials com una transmissió d'esdeveniments
 - XII. Administració de processos Executar les tasques de gestió / administració com a processos que només s'executen un cop

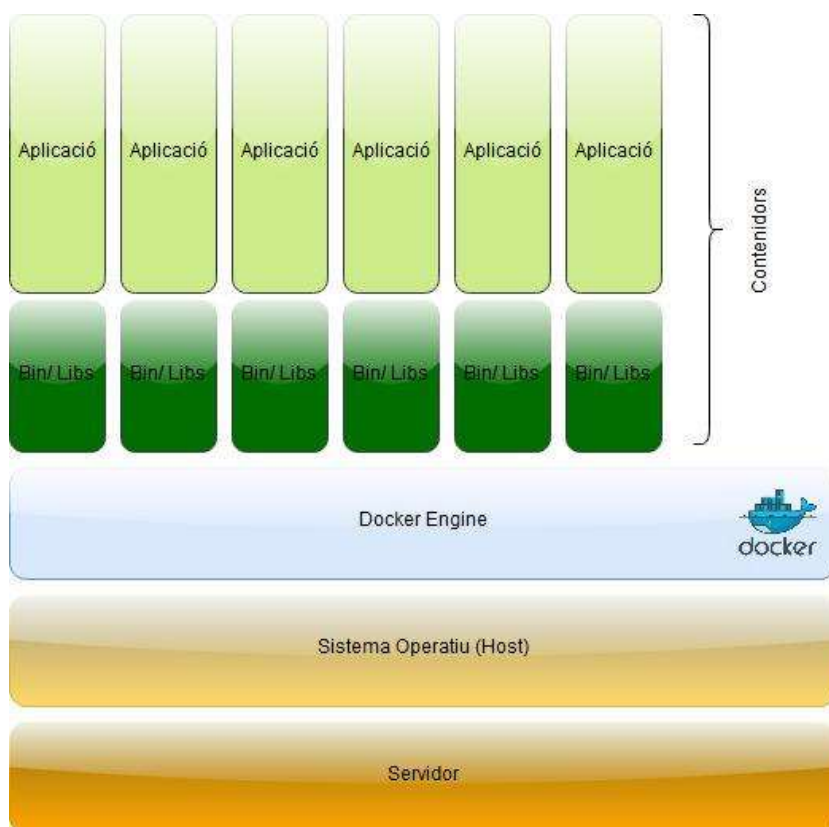
En essència es tracta d'establir un contracte clar amb el sistema operatiu, de forma que les aplicacions tinguin màxima portabilitat, puguin escalar, no tinguin dependències fortes amb una instància concreta (fitxers), i minimitzin les diferències amb l'entorn de desenvolupament.

Els processos d'aplicació no poden tenir estat, i s'executen en mode anomenat "shared-nothing". Qualsevol informació d'estat s'ha d'emmagatzemar en un servei extern, mai en local.



18.3.2. Preparada per a ser desplegada en qualsevol cloud

- Es pretén que les aplicacions estiguin llestes per a ser desplegades al servidors clàssics, però també al núvol, ja sigui privat, públic o mixt. Per complir aquest objectiu, s'acabi desplegant en l'entorn de contenidors o no, caldrà orientar el desenvolupament al seu desplegament en contenidors, preparant l'aplicació per al seu funcionament a la infraestructura productiva. Per això es partirà d'imatges preparades per l'IMI que s'hauran de fer servir de base per a la construcció de les imatges definitives que caldrà desplegar.
- Objectius d'aquesta orientació:
 - Igualar els entorns el màxim possible.
 - Simplificar la Instal·lació: En fer servir imatges mestres preparades a tal efecte.
 - Independitzar-se de la plataforma: Les imatges amb els contenidors es poden canviar d'un sistema a un altre facilitant no només els canvis en l'àmbit productiu sinó les proves a entorns locals o de desenvolupament.
 - Aïllar les aplicacions: Cada aplicació pot o no compartir contenidors de forma que es poden aïllar segons les necessitats existents.
 - Automatitzar l'administració.



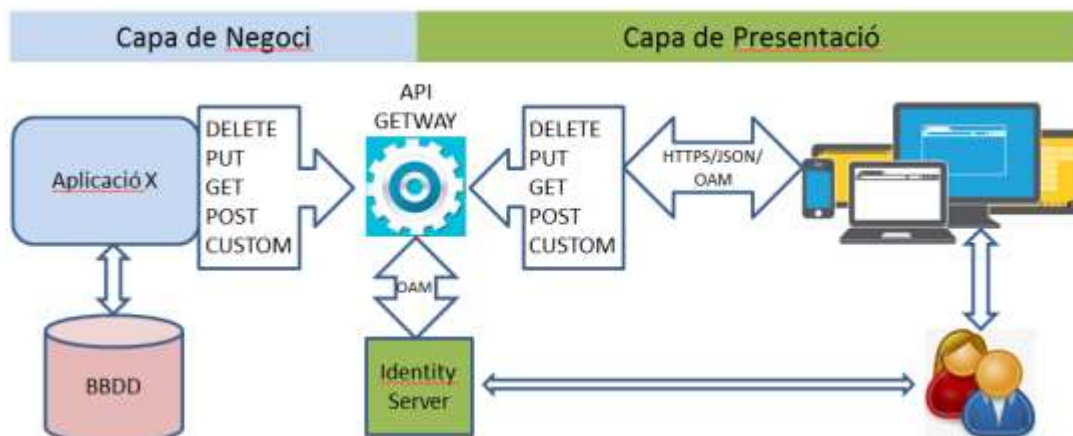


18.4. Modularitat i escalabilitat

Per eficiència i sostenibilitat el sistema a construir haurà de ser modular i escalable: ha de tenir un enfocament prou transversal per a minimitzar l'impacte de la incorporació de noves funcionalitats.

18.4.1. Arquitectura Modular

Com a mínim tota aplicació tindrà 2 instal·lables*: Serveis (Negoci que es publicarà a l'API Gateway) i el client (Presentació). La imatge de sota il·lustra com interactuen AQUESTS components.



Serveis (Negoci)

- L'instal·lable haurà de seguir una arquitectura de "monòlit modular" no pas de *microserveis*.
- Es farà una divisió en instal·lables de l'aplicació basada en funcionalitats. Cadascun d'aquests instal·lables donarà compliment a uns requisits funcionals concrets de l'aplicació.
- Els serveis s'implementaran RESTful sense sessió al costat del servidor proporcionant:
 - Consultes de les entitats del model de dades.
 - Manteniment de les entitats del model de dades.
 - Funcionalitats de negoci.
- Per consumir serveis comuns d'altres aplicacions s'utilitzarà els serveis publicats a l'API Manager. Aquests serveis es diferencien en dos tipus:
 - Serveis públics, només cal tenir un clientId per consumir-los.
 - Serveis privats o autenticats, cal autenticació amb un usuari (nominal o de servei) per tal de poder consumir el servei.
 - Això comporta fer una autenticació amb l'usuari per obtenir un token i enviar aquest token en totes les crides al servei junt amb el clientId.
- Les API(s) es publiquen a l'API Manager sense excepció i no poden ser consumides fora d'ell.



18.4.2. Publicació a l'API Manager

- Cal especificar el/s servei/s en un fitxer swagger (format yaml) per tal de publicar-lo a l'API Manager
- Aquesta publicació té entitat pròpia i requereix tenir-la en compte al projecte.

18.4.3. Frontals o Clients (Presentació)

- Cada aplicació disposarà d'una capa de presentació per generar la GUI dels usuaris.
- La capa de presentació és la responsable de generar les pantalles a l'usuari i d'atendre les seves peticions. No ve fixada pel framework del IMI.
- Pot estar basada en el framework estàndard per a aplicacions SPA de l'IMI: Arquitectura Angular5 + Bootstrap com framework de presentació. És responsable de generar les pantalles a l'usuari i d'atendre les seves peticions.
- No té a dins llibreries ni per resoldre funcionalitats de negoci ni per accedir directament a base de dades ni per accedir als elements tercers a integrar.
- Totes aquestes funcionalitats les delega en l'aplicació de la capa negoci descrita abans cridant a les seves API(s) RESTful.
- Les API(s) es consumeixen mitjançant l'API Manager, mai directament.
- L'aplicació s'integrarà amb els serveis amb la seguretat corresponent (mireu l'apartat de seguretat).
- Si es fa servir la presentació SPA inclosa en el framework (**no és obligatòria**):
 - Farà servir el conjunt de controls visuals per aplicacions de la Intranet de l'Ajuntament, inclosos al framework, adaptats a la guia d'estils per aplicacions de la Intranet de l'Ajuntament.
 - Proporciona un entorn de desenvolupament Local:
 - Un instal·lador per a les eines següents.
 - nvm (si es prepara per desenvolupar en linux) o nvm-windows o nodist (si es prepara per desenvolupar en MS Windows).
 - Visual Studio Code.
 - Preconfiguració per forçar la versió de Node.js decidida per l'IMI.

Frontals o Clients Web (SPA)

- HTML5
- Disseny responsiu
- A ser possible basat en bootstrap
- Utilització de llibreries de javascript de solvència contrastada
- Interfícies riques d'usuari (jQuery o Vue.js)
- Compressió de css i js en els mínims fitxers possibles
- Less o Sass com a llenguatges d'estils
 - Traducció de less/sass a CSS en temps de construcció, per part del procés de desplegament (no en viu).



18.4.4. Estructura multi-idioma

La solució ha de ser multi-idioma. La totalitat dels camps/missatges visibles per l'usuari han de poder traduir-se a taules, de manera que la incorporació d'un o un altre idioma no suposi haver de revisar i traduir codi font. El multi-idioma aplica als *tags* associats a llistats, pantalles i documents així com als missatges que generi el sistema en les diferents pantalles, incloent pantalles d'ajuda. El multi-idioma no aplica al contingut de la base de dades (informació associada al *data entry*).

L'IMI requereix que l'aplicació vingui configurada inicialment en català, si bé es demanarà la visualització d'un parell de pantalles, documents, llistats i missatges en castellà per comprovar el correcte funcionament de la característica multi-idioma del sistema construït. La documentació que es generi en el transcurs del contracte només s'haurà d'entregar en català.

18.5. Directives a tenir en compte tant en l'adquisició de software com en el desenvolupament a mida

18.5.1. Traçabilitat

Adicionalment, el sistema haurà de garantir la traçabilitat de les accions dels usuaris sobre el mateix.

18.5.2. Components de software lliure

L'IMI advoca per reduir el nombre de components de software amb llicència, i recomana per tant l'ús de components de codi obert.

18.5.3. Stages

L'IMI disposa de 4 entorns per a l'execució d'aplicacions:

- **Entorn local:** el desenvolupament es fa en el PC del desenvolupador. Aquest entorn permet fer totes les proves i integracions necessàries del producte.
- **Entorn d'integració:** en aquest entorn s'instal·len en primera instància les aplicacions. Permet identificar els errors d'integració amb els components de l'arquitectura de l'IMI.
- **Entorn de pre-producció:** una vegada depurats els errors d'integració, les aplicacions s'instal·len en aquest entorn. És idèntic a l'entorn de producció i permet comprovar que les aplicacions funcionaran correctament quan s'instal·lin en producció.
- **Entorn de producció:** aquest és l'entorn definitiu en què treballa l'usuari i on s'han de deixar instal·lades les aplicacions.

Totes les aplicacions lliurades a l'IMI s'han d'instal·lar, posar en funcionament i provar en aquests quatre entorns si no es pacta altre cosa durant el desenvolupament del projecte.



18.5.4. Usabilitat

- Com a criteri general, s'ha de separar el contingut de la presentació, ajustar-se a l'especificació CSS 2.1 del W3C (World Wide Web Consortium) utilitzant les Fulles d'Estil proporcionades per l'Ajuntament de Barcelona. Per aconseguir aquest objectiu s'han de complir els requisits i consideracions definides a les guies d'estil de l'Ajuntament.
- La presentació s'ha de visualitzar correctament amb els navegadors Firefox vers 69 o posteriors.
- El temps d'aprenentatge del sistema per un usuari haurà de ser menor a 4 hores.
- El sistema disposarà de manuals d'usuari estructurats adequadament.
- El sistema ha de proporcionar missatges d'error que siguin informatius i orientats a usuari final.
- El sistema haurà de disposar d'un mòdul d'ajuda en línia.
- L'aplicació Web ha de posseir un disseny "Responsive" i Multidispositiu, a fi de garantir l'adequada visualització a múltiples dispositius: DeskTop, Tauletes i Telèfons Intel·ligents.
- Si existeix el requeriment d'utilització de l'aplicació en dispositius mòbils, caldrà desenvolupar l'aplicació com a una PWA (Progressive Web Application).

18.5.5. Eficiència

- Tota funcionalitat del sistema i transacció de negoci ha de respondre a l'usuari en menys de 3 segons en el 90% de les peticions. I podem afegir la següent informació a tenir en compte:
 - 0.1 segons és el límit perquè l'usuari senti que el sistema reacciona instantàniament, és a dir, que no es necessita cap retroalimentació especial, excepte per mostrar el resultat.
 - 1-3 segons és el límit del flux de pensions de l'usuari per mantenir-se ininterrompuda, tot i que l'usuari observarà el retard. Normalment, no es necessita cap retroalimentació especial durant els retards de més de 0,1, però inferiors a 1,0 segons, però l'usuari perd la sensació d'operar directament sobre les dades.
 - 10 segons és el límit per mantenir l'atenció de l'usuari centrada en el diàleg. Per a retards més llargs, els usuaris hauran de realitzar altres tasques mentre espera que acabi l'ordinador, de manera que se'ls hauria de proporcionar informació que indiqui quan s'espera que l'ordinador es faci. La retroalimentació durant el retard és especialment important si el temps de resposta és molt variable, ja que els usuaris no saben què esperar.
- El sistema ha de ser capaç d'operar adequadament amb fins a XXXX usuaris amb sessions concurrents.
- El sistema ha de ser tolerant a errors.
- El sistema ha de garantir la integritat de les transaccions.



18.5.6. Seguretat de l'aplicació

El component de seguretat de la plataforma s'ha de tenir sempre present. L'arquitectura té en compte no tan sols la millor manera d'estructurar l'aplicació, sinó que aquesta estructura ha de complir amb els requisits de seguretat de l'Ajuntament. En aquests moments aquests requeriments marquen que s'hagi de diferenciar entre l'accés a les dades extern, que es faria mitjançant un API i l'accés ja dins la xarxa que es farà cap a la base de dades. L'objectiu de seguretat és poder controlar millor l'accés a les dades mitjançant el control dels tallafocs i l'accés a la base de dades.

Arquitectures possibles

En general es farà servir una arquitectura que s'ha anomenat 4bis per a la construcció de les aplicacions. Aquesta arquitectura està consensuada amb el departament de seguretat de l'Ajuntament i representa un compromís entre seguretat i complexitat.

Distingim tres blocs d'aplicacions:

Aplicacions públiques

Són aquelles que seran utilitzades pel ciutadà, que no requereixen d'autenticació o no utilitzen l'autenticació de l'Ajuntament.

Aquestes aplicacions poden exposar una web o una API a través d'una o varies apps Django. El frontal mai accedirà directament a la base de dades i serà l'APP la responsable de la connexió.

Aplicacions privades

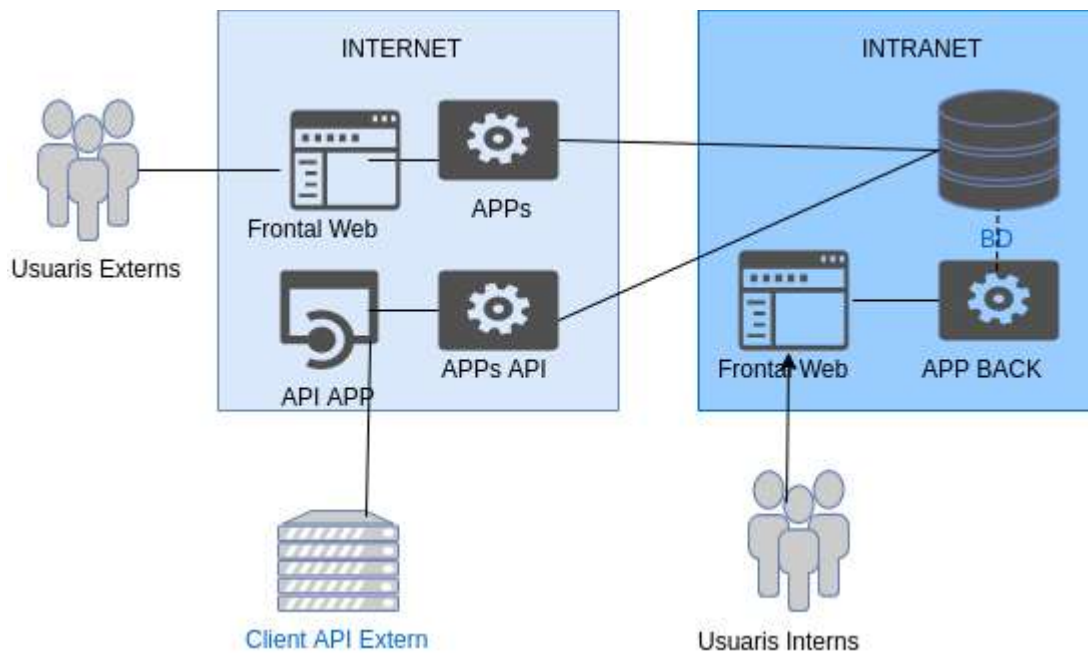
Són aquelles en les quals sols es té accés dins la xarxa interna de l'Ajuntament o bé que accedint-se via Internet necessiten d'un usuari autenticat per l'Ajuntament. Poden exposar un frontal web, normalment un backoffice o una API. L'autenticació dels usuaris de l'aplicació es fa mitjançant LDAP o Directori Actiu.

De la mateixa manera que a les aplicacions públiques, mai s'accedeix des de la capa de presentació a la base de dades.

Aplicacions totals

Són aplicacions que tenen tant un component públic com un component privat. S'apliquen les consideracions dels dos models anteriors.

A continuació es presenta un esquema complet.



- **Autenticació:** El sistema ha de comprovar que l'usuari que tracta d'accedir al sistema és qui diu ser. De forma general, l'autenticació dels usuaris es pot fer mitjançant els següents mecanismes:
 - Usuari i contrasenya validada contra un servidor de credencials corporatiu.
 - Aquest requeriment es realitzarà mitjançant la utilització del sistema d'Autenticació i Autorització corporatiu.
- **Autorització:** El sistema ha d'implementar mecanismes per a restringir a usuaris no identificats i autoritzats l'accés a la informació. Aquest requeriment es realitzarà mitjançant la utilització del sistema d'Autenticació i Autorització corporatiu.
- Es farà coincidir els usuaris d'aquest sistema amb els usuaris de la xarxa corporativa i evitant la reinserció de credencials (SSO). Aquest requeriment es realitzarà mitjançant la utilització del sistema d'Autenticació i Autorització corporatiu.
- **Xifrat de dades:** La comunicació de l'usuari amb el sistema es realitzarà únicament mitjançant canals segurs (https). Els algorismes criptogràfics emprats seran els acreditats pel Centre Criptològic Nacional per al seu ús en l'Esquema Nacional de Seguretat.
- **Gestió d'usuaris i sessions:** Els mecanismes de control de sessions d'usuaris autenticats contemplaran:
 - Tancament de sessió per part de l'usuari.
 - Expiració automàtica de sessió.
- **Gestió d'errors i excepcions:** Es realitzarà un tractament sistematitzat i centralitzat d'errors i excepcions, eliminant la informació interna del sistema o sensible dels missatges mostrats a l'usuari.
- El nou sistema s'ha de desenvolupar seguint patrons i recomanacions de programació que incrementin la seguretat de les dades.



- Qualsevol intercanvi de dades entre serveis o aplicacions es realitzarà mitjançant API(s) de serveis fen servir el protocol encriptat HTTPS.
- Les dades que formin part d'un fitxer de nivell ALT segons la LOPD seran encriptades. No es guardaran de forma oberta a la BD i només es desencriptaran per ser llegides un cop comprovat que l'usuari té el perfil necessari per veure-les.
 - L'IMI indicarà quin algoritme s'ha de fer servir en cada cas.

18.6. Qualitat

18.6.1. Codi

- Codificació: UTF-8
- Indentació: amb 4 espais
- Longitud màxima de línia 119 caràcters.
- Cal fer servir eines de validació (com per exemple PyLint en el cas de python)

Idioma

- El codi, els comentaris que s'afegeixen al codi, el nom de les variables o altres components del codi, així com documentació tècnica (no d'usuari), s'han d'escriure en anglès.
- Per contra, els paths de les URLs de l'aplicació i de les APIs, s'han d'escriure en català, ja que són part visible per l'usuari de l'aplicació.

18.6.2. Qualitat de codi

- Tot codi font que es vulgui desplegar als servidors de l'IMI requerirà el compliment dels estàndards de qualitat indicats pel mateix IMI. Aquests estàndards es concreten en l'aplicació de diferents Quality Gates.
- El conjunt de regles de qualitat de codi de l'eina SonarQube (es revisen/actualitzen anualment). [actualment ver. 8.4].
- En cap cas les conseqüències del no compliment d'aquests estàndards podrà justificar l'endarreriment de les fites d'entrega del projecte.

Aplicacions antigues

- En cas d'aplicacions antigues, no desenvolupades des del seu inici amb els actuals llistats de qualitat, es marquen llistats de qualitat diferents.
- En qualsevol cas el proveïdor es compromet a no empitjorar el nivell de qualitat actual de l'aplicació. Això implica que el nou codi desenvolupat no empitjorarà els següents indicadors:
 - Número de Bugs
 - Número de Vulnerabilities
 - Security Hotspots
 - Security Rating
 - Technical Debt Ratio



- Pel que fa a les proves unitàries. L'IMI podrà exigir que el nou codi compleixi amb la regla del 60% de Cobertura. No obstant això, el proveïdor podrà demanar la relaxació d'aquest llindar justificant la seva complexitat en vers l'estat del desenvolupament.
 - Aquesta justificació haurà de ser aprovada per la direcció de projecte, arquitectura i seguretat.
 - En cap cas aquest nou llindar serà inferior al 30% de Cobertura de codi.

Quality Gates per tecnologies:

Java:

- Conditions on New Code
 - **Coverage**, ha de ser superior al 30.0%
 - **Bugs**, no es permet cap bug
 - **Vulnerabilities**, no es permet cap vulnerability
- Conditions on Overall Code
 - **Blocker Issues**, no es permet cap.
 - **Coverage**, ha de ser, com a mínim, del **60.0%** de tot el codi del projecte
 - **Critical Issues**, no es permet cap.
 - **Unit Test Failures**, 0. Tots els test case han funcionar.

Python:

- Conditions on Overall Code
- **Blocker Issues**, no es permet cap.
- **Coverage**, ha de ser, com a mínim, del **30.0%** de tot el codi del projecte

El conjunt de regles és el que ve amb la versió de Sonarqube indicada.

18.6.3. Qualitat del producte final

S'aconsella l'ús de desenvolupament dirigit per tests (*test driven development*) que possibiliti la instal·lació d'un sistema d'integració continua.

Es tracta d'una metodologia de desenvolupament de software, basada principalment a garantir la qualitat del codi, i la qual s'empra en un breu cicle que es repeteix durant tot el desenvolupament. Aquest cicle és:

1. Es prenen els requisits a desenvolupar.
2. Els requisits es converteixen en tests (abans de començar a codificar).
3. Es passa la bateria de tests ja creats i es comprova que els nous tests efectivament donen error.
4. Es desenvolupen els nous requeriments per a satisfer aquests nous tests.
5. Es passa novament la bateria de tests, i es comprova que tots queden satisfets.
6. Es refactoritza el codi per adaptar les noves funcionalitats, cohesionant-les amb la bateria de test anterior.
7. Es torna al punt 1 si encara no s'ha acabat el producte.



Els beneficis de seguir aquesta metodologia són els següents:

- La bateria de tests es manté sempre actualitzada.
- El projecte esdevé robust i auto documentat.
- El producte final és més fidel als requisits presos.
- Detecció ràpida de desviacions en el desenvolupament.
- Millora de la qualitat del producte final.
- Minimització del temps dedicat a la depuració d'errors.
- Minimització del temps dedicat a la fase de manteniment.
- Garantia de mínim impacte en la implementació de noves funcionalitats.
- Els tests han de complir una sèrie de requisits:
- Han de ser auto descriptiu sobre la funcionalitat que estan provant.
- Han de servir com a documentació del codi.
- Han de ser tan unitaris com sigui possible.
- No han de dependre d'altres tests.
- Han de partir d'un escenari concret i deixar els recursos alliberats tal com els van trobar en iniciar l'escenari.
- La cobertura dels tests ha de ser tan completa com sigui possible: les funcionalitats s'han de provar en tots els casos plausibles d'esdevenir.

El tipus de tests que es desenvoluparan seran els següents:

- Tests unitaris: sobre cada classe / funcionalitat a desenvolupar.
- Tests d'integració: sobre les integracions dels diferents components entre les seves interfícies. Si els components són externs (APIs, *webservices...*), se simularà aquest i la seva interacció mitjançant *mockups*.
- Tests d'interfície d'usuari: aquests ens serviran per garantir que la interfície d'usuari és robusta i completa segons les especificacions.
- Tests de rendiment: amb aquests tests garantirem que el sistema és escalable sobre els recursos proporcionats, amb un rendiment acceptable, proposat en el projecte.
- Tests de regressió: verifica que els canvis aplicats al producte no tenen cap impacte negatiu en les característiques que anteriorment funcionaven correctament.

S'hauran de seguir aquestes bones pràctiques:

- L'estructura del test ha de dividir-se en les següents parts:
 - Inicialització: inicialitzem l'entorn tal com el necessitem per executar el test.
 - Execució: executem les funcionalitats desitjades amb el flux adequat.
 - Validació: validem que els resultats de l'execució coincideixen amb els resultats esperats.
 -
 - Neteja: eliminem el rastre d'execució del test.
- Quan es comprova funcionalitats dependents de tercers (APIs, *webservices...*) és una bona pràctica l'ús de *mockups* per no afectar el sistema finalista.



Proposta de redactat

Els licitadors han de presentar una proposta de gestió de flux general de desenvolupament en el conjunt de documentació tècnica que es detalla al punt "Proposta Tècnica", amb el detall suficient que permeti la valoració de la facilitat d'aplicació de la proposta i l'optimització de les iteracions i l'assegurament de la realització de les seves tasques.

18.7. Metodologia de desenvolupament

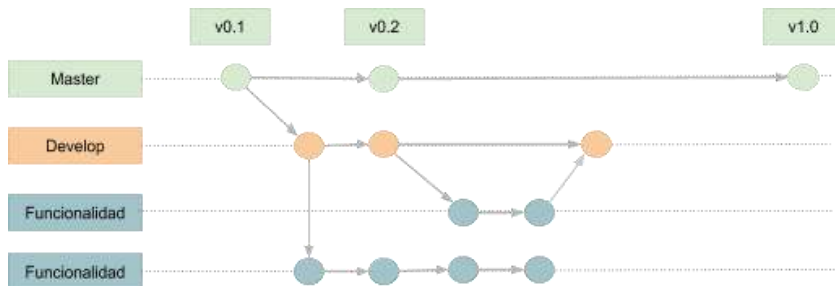
- L'empresa adjudicatària haurà de gestionar 4 entorns per a l'execució d'aplicacions: desenvolupament, integració, pre-producció i producció.
 - Entorn local: el desenvolupament es fa en el PC del desenvolupador. Aquest entorn permet fer totes les proves i integracions necessàries del producte.
 - Entorn d'integració: en aquest entorn s'instal·len en primera instància les aplicacions. Permet identificar els errors d'integració amb els components de l'arquitectura de l'IMI.
 - Entorn de pre-producció: una vegada depurats els errors d'integració, les aplicacions s'instal·len en aquest entorn. És idèntic a l'entorn de producció i permet comprovar que les aplicacions funcionen correctament quan s'instal·lin en producció.
 - Entorn de producció: aquest és l'entorn definitiu en què treballa les persones usuàries i on s'han de deixar instal·lades les aplicacions desenvolupades (mòduls i funcionalitats). Totes les aplicacions lliurades a l'Ajuntament de Barcelona s'han d'instal·lar, posar en funcionament i provar en aquests entorns.
- L'aplicació ha de ser configurada perquè pugui integrar-se amb *Sentry*, o sistema similar, per a la monitorització d'errors en l'àmbit d'aplicació.
- És necessari que el producte s'entregui de manera que sigui possible un desplegament basat en automatització per mitjà de contenidors en màquines de tipus *Ubuntu/Debian*.

18.8. Repositori de codi

- Per gestionar el codi es farà servir el gestor de codi corporatiu de l'Ajuntament, actualment GIT (<https://gitlab.ajuntament.bcn/>).
- Els canvis en el codi hauran de pujar-se a través de *Pull Requests* al repositori de codi, on un mínim d'una persona de l'equip del servei de l'empresa adjudicatària hauran de revisar el codi i aprovar els canvis.
- És responsabilitat de l'empresa adjudicatària garantir que es puguin disposar en el mateix repositori de:
 - El codi de l'aplicació.
 - La llista de dependències amb altres llibreries i aplicacions lliures.
 - Els fitxers de generació de contenidors Docker si no fan servir els estàndards de desenvolupament en Java o Python.
- Com a mínim es faran servir dues branques estables:
 - *develop* -> Continuarà el codi provat i finalitzat per desplegar a l'entorn d'integració.



- master -> Continuarà el codi provat i finalitzat per desplegar a pre-producció. Un cop validat a pre-producció ja no hi haurà més construccions. Aquesta construcció validada serà la que s'instal·larà a producció.
- Cada nova implementació es farà en una nova branca i s'integrarà a la branca oficial quan es consideri provat i estable.
 - Esquema de funcionament:



18.9. Construcció i desplegament

Els desenvolupaments han d'orientar-se cap a processos que ens permetin la construcció, proves i desplegament d'aplicacions de manera automatitzada per tal de poder disminuir els cicles de desenvolupament-proves-validació-posada a producció.

Per una altra banda s'ha de garantir la traçabilitat del codi que es posi en producció i això vol dir fer un ús intensiu dels sistemes de control de versions (git) i d'eines de desplegament automatitzat, de manera que es pugui garantir que el codi que hi ha als servidors correspon a la versió que volem i que no ha estat manipulat.

18.10. Llicències

Els desenvolupaments que es facin són propietat de l'Ajuntament i s'han de llicenciar de tal manera que l'Ajuntament tingui la llibertat de publicar el codi sota la llicència que consideri més adient. Cal consultar la guia per gestionar projectes de programari lliure de l'Ajuntament de Barcelona per obtenir més informació d'aquest tema:

<https://ajuntamentdebarcelona.github.io/foss-guide/ca/Introduccio.html>



19. ANNEX 7: NORMATIVA PYTHON

19.1. Introducció

Aquest document pretén ser una guia de referència per al desenvolupament d'aplicacions Python a l'IMI. Hem de tenir en compte que aquest document només fa referència a les particularitats pròpies de Python que no han sigut mencionades a l'Annex 6.

Tant l'arquitectura proposada com el mètode de desplegament s'entenen adaptables a les circumstàncies de cada aplicació i entorn on aquest s'hagi de desplegar. Com diu un dels lemes del Zen Python

*Special cases aren't special enough to break the rules.
Although practicality beats purity.*

S'ha d'entendre que encara que s'han de procurar seguir aquestes regles per tenir una arquitectura escalable, mantenible i gestionable, cada aplicació és un món i s'ha d'arribar a un compromís entre el seguiment total de les regles i el poder donar servei.

19.2. Arquitectura bàsica

En essència es tracta d'establir un contracte clar amb el sistema operatiu, de forma que les aplicacions tinguin màxima portabilitat, puguin escalar, no tinguin dependències fortes amb una instància concreta (fitxers), i minimitzin les diferències amb l'entorn de desenvolupament.

Els processos d'aplicació no poden tenir estat, i s'executen en mode anomenat "shared-nothing". Qualsevol informació d'estat s'ha d'emmagatzemar en un servei extern, mai en local.

19.2.1. Codi

En aquest document no es recomana un IDE concret de desenvolupament: atom, vscode, PyCharm, Vim, Eclipse, etc. són IDEs de programació prou coneguts i que permeten ser configurats sense problemes per fer servir Python.

El requeriment fonamental que s'haurà de seguir és:

- Intèrpret Python: 3.x, preferiblement la versió 3.7, la utilització de la branca 2.7 s'hauria de justificar de manera adient.
- El codi ha de validar a PEP8, de manera que el format del codi sigui comú per a tots els projectes.

És convenient a més dels tests unitaris que s'apliquin passar una eina de validació com PyLint per a detectar possibles errors del codi i que aquests estiguin dins el procediment de construcció previ al pas a producció.



Tant a desenvolupament com als entorns de test, preproducció i producció, la instal·lació del codi i les llibreries s'ha de fer dins l'àmbit d'un *virtualenv*, per tal de tenir control sobre quines llibreries s'utilitzen i fins i tot sobre quina versió de Python executarà el codi. En el cas de desplegament sobre *docker*, no fa falta *virtualenv* ja que tot el contenidor Python està dedicat a l'aplicació.

19.2.2. Components

Les llibreries i components que es llisten en aquest document representen un recull que amb l'experiència de projectes Django acumulada són les millors opcions en aquests moments per resoldre una sèrie de problemes concrets. En cap cas es farà menció a una versió concreta, ja que això implicaria no mantenir-los actualitzats.

La llista de components no és exhaustiva i ha de servir per a que, en cas d'haver de resoldre un problema, s'opti per una de les llibreries proposades enlloc de cercar-ne una de nova i dificultar així les tasques de manteniment. La idea és que s'hagi de justificar el perquè es resol un problema amb una de les llibreries no estàndard.

En el cas de **paquets i llibreries externes** l'opció preferida és que aquestes estiguin dins el repositori PyPi. Si per alguna raó una llibreria no hi és i s'ha d'agafar de Github, llavors s'ha de fer un fork de la mateixa per garantir que estarà disponible en el futur.

19.2.3. Construcció i desplegament

Els desenvolupaments han d'orientar-se cap a processos que ens permetin la construcció, proves i desplegament d'aplicacions de manera automatitzada per tal de poder disminuir els cicles de desenvolupament-proves-validació-posada a producció.

Per una altra banda s'ha de garantir la traçabilitat del codi que es posi en producció i això vol dir fer un ús intensiu dels sistemes de control de versions (*git*) i d'eines de desplegament automatitzat, de manera que es pugui garantir que el codi que hi ha als servidors correspon a la versió que volem i que no ha estat manipulat.

19.3. Seguretat

En el que fa referència a aquest document, els requeriments de seguretat impliquen anar actualitzant tant l'aplicació com els mòduls que es facin servir amb els darrers pegats de seguretat, especialment en el que fa referència al *core* de Django.

19.4. Directrius de Desenvolupament

El desenvolupament d'aplicacions Python/Django es pot fer seguint un model clàssic on les vistes es desenvolupen com a funcions, o bé amb un model d'orientació a objectes, on les vistes són classes també. Es donarà preferència al model orientat objectes vers el model basat en funcions.

[DP1]. Inici del projecte. Es recomana la utilització d'una eina com *cookiecutter* o semblant per muntar d'inici l'estructura de projecte, de manera que amb aquesta plantilla ja es creï



una estructura d'aplicació comuna. Per tal de facilitar el desplegament de l'aplicació convé que l'arxiu de `settings.py` i `wsgi` estigui a un lloc conegut que no depengui del nom del projecte. Proposem `main` com a nom del paquet que contingui aquests arxius. L'estructura base quedaria com:

```
nom_del_projecte
  README.rst
  bin
  src
  main
  settings.py
  wsgi.py
  ...
  ...
  ...
```

La utilització de `cookiecutter` no és obligatòria, mentre es compleixi l'estructura de directoris i fitxers explicada.

[DP2]. Lògica de negoci. Utilitzarem l'aproximació de *fat models*, és a dir, la lògica de negoci la posarem preferentment als models, als formularis i a llibreries externes. Procurarem que el component *views* sols gestioni la part de lògica de presentació.

[DP3]. Middleware i context processors. S'ha de procurar mantenir optimitzada tant la capa de *middleware* com el context comú que es passa dins cada *request*. Evitarem passar informació que no necessitem i no carregar el processament de les *request* si no és estrictament necessari, ja que això va en detriment del rendiment de l'aplicació.

[DP4]. Fulles d'estil. Es recomana la utilització de pre-processadors com SAAS o LESS. La creació dels CSS a partir dels fitxers SAAS o LESS. Disposem d'una aplicació pròpia anomenada *dtiassets* que ja inclou plantilles, estils, formularis, etc. predefinits.

[DP5]. Sessions. Les sessions es guardaran en base de dades fent-ne *caché* cap a Redis/Memcached. Quan les sessions no necessitin persistència no farà falta guardar-les a base de dades. Per gestionar els logins mitjançant LDAP, disposem d'una app anomenada *ldapdti*.

[DP6]. Catxé. Utilitzarem Redis com a sistema de *catxé* preferit en configuració de no escriptura a disc. Redis ens permet tenir diferents bases de dades dins el mateix servidor i poder eliminar claus completament o per blocs, donant-nos un control molt més fi que Memcached, que seria l'alternativa en cas que no es pugui fer servir. Es pot utilitzar Varnish i CDN per accelerar també la càrrega de contingut.

[DP7]. API. Django Rest Framework (DRF) és l'opció recomanada per a la creació d'APIs per a les nostres aplicacions. Les APIs aniran versionades de manera que es pugui mantenir l'API anterior encara que se'n creï una de nova.



[DP8]. Gestió de *media*. Entenem per *media* els fitxers produïts durant l'ús de l'aplicació per part dels usuaris, i que formen part del model de dades. Per exemple, imatges pujades per usuaris. No podem suposar que els contingut d'imatges i multimèdia pujats pels usuaris estaran al servidor que executa el procés de l'aplicació. Es recomana la utilització d'un servei com S3 o compatible amb S3. D'aquesta forma, un procés desplegat a una instància es pot aturar i llançar a una altra, sense tenir cap dependència amb fitxers locals.

[DP9]. Gestió d'estàtics. Entenem per estàtics tots els fitxers creats pels desenvolupadors, com a javascript, css o imatges per a maquetació. Els estàtics han de ser immutables durant tota la vida del procés. Un procés no pot canviar els seus estàtics (per exemple minimitzar javascript, pre-processar less, o crear *thumbnails* d'imatges) durant el seu cicle de vida. Els estàtics són per tant un artefacte produït al moment de "*build*", i immutable durant el desplegament. Recomanem que siguin servits des d'un servei dedicat (nginx), o CDN. En el cas d'usar contenidors docker, els estàtics són produïts al cicle de *build*, usant l'aplicació *staticfiles* de *django*, amb *collectstatic*. En el cas de fer servir una utilitat com a Django Compressor, s'ha d'habilitar la compressió *offline*, també durant el cicle de *build*.

[DP10]. Thumbnails i redimensionament d'imatges. Sempre que sigui possible s'utilitzarà un servei extern com Thumbor per a redimensionar les imatges que s'hagin de servir amb unes dimensions diferents de les que ha pujat l'usuari. Amb això descarregarem el processament de la imatge del procés principal que ha de servir els continguts i evitarem l'efecte bloqueig.

[DP11]. Javascript. Per aplicacions que facin ús moderat de Javascript, recomanem utilitzar jQuery i jQuery UI, amb l'opció d'afegir altres frameworks com Vue.js. Per contra, si s'està desenvolupant una SPA, utilitzarem ES6 sempre que sigui possible i recomanem la utilització de Vue.js o AngularJS.

[DP12]. Monitorització d'excepcions de codi. S'ha d'utilitzar un servei de monitorització de les aplicacions de manera que tinguem informació automàtica dels errors no previstos que s'han produït. Django per defecte ens proveeix d'una configuració mínima, però és convenient utilitzar Sentry per això, ja sigui en mode intern amb una instància dedicada, o bé, utilitzant serveis de cloud.

[DP13]. Configuració de l'aplicatiu. Seguint la filosofia 12factor, la configuració de l'aplicació no pot estar a foc dins l'arxiu *settings* i s'han d'utilitzar variables d'entorn per totes aquelles variables de configuracions que depenguin de l'entorn de desplegament, per exemple: base de dades, *secret_key*, *catxé*, etc.

És a dir, totes les variables de configuració que han de canviar (o poden canviar) entre diferents entorns (prod, pre, test), han de ser configurables via variables d'entorn.

Això inclou la definició de serveis externs (redis, base de dades, bucket S3), i altres com claus secretes.

[DP14]. Tasques batch.



Distingirem dos tipus de tasques *batch*, aquelles periòdiques que s'executen a hores concretes i aquelles que s'inicien mitjançant l'acció de l'usuari o sistema.

Tasques a hores concretes.

Per aquestes tasques periòdiques senzilles podem fer servir la utilitat *cron*: un procés que llegeix un calendari en format predefinit (*crontab*) i executa els processos periòdicament. Una alternativa és utilitzar *celery* pels crons. En aquest cas s'ha d'avaluar si el projecte ja té *workers*.

Tasques iniciades per un esdeveniment d'usuari o aplicació

Per tasques més complexes, amb dependències, o que es generen a partir d'esdeveniments d'usuari durant l'execució de la aplicació, és convenient la utilització d'un sistema de cues. El sistema de cues escollit dependrà de la complexitat de les tasques a coordinar, recomanant-se anar a sistemes que van de menys a més complexitat.

[DP15]. Requeriments. La llista de llibreries i les seves versions que s'utilitzin a l'aplicatiu han d'anar dins la carpeta *requirements* i s'especificarà la versió concreta que es fa servir. En cas de desplegament en contenidors a més s'afegiran fitxers per indicar les llibreries de sistema operatiu a instal·lar. Per exemple:

```
requirements
base.txt
production.txt
dev.txt
system-production.txt
system-dev.txt
```

- *requirements/base.txt*: Dependències de Python comunes que s'utilitzen a tots els entorns. És el gruix dels requeriments del projecte.
- *requirements/production.txt*: Dependències de Python que només es necessiten a producció. Ha d'incloure *base.txt*
- *requirements/dev.txt*: Dependències de Python per al desenvolupament en local i per executar els tests.
- *requirements/system-production.txt*: Dependències de sistema operatiu (paquets *apt*) necessàries en execució
- *requirements/system-dev.txt*: Dependències de sistema operatiu (paquets *apt*) necessàries en el moment de construcció

Si es necessita afegir una llibreria precompilada que no es pot obtenir de les fonts oficials de *pip* s'introduiran a la carpeta *wheels* del projecte i s'hi farà referència des dels fitxers de *requirements* anteriors.

19.4.1. Implementacions

A la taula següent es llisten una sèrie d'eines d'ús comú en la majoria d'aplicacions Django que es desenvolupen.



Eina	Referència	Observacions (Descripció / Casos d'ús / Alternatives)
Python-decouple	DP13	Permet definir configuracions (settings) basats en variables d'entorn. També es permet utilitzar fitxers .env
Crons	DP14	Definir tasques periòdiques que no tenen molts requeriments de memòria. Les tasques es poden gestionar mitjançant comandes de Django (management commands), si el nombre de tasques augmenta o hi ha dependències entre tasques, s'ha de passar a un sistema de cues dedicat basat en Celery o Django RQ.
Celery i Django RQ	DP14	Sistema de cues. Si el projecte té una gran complexitat, llavors es pot plantejar la introducció de Celery, sinó també es podria utilitzar Django RQ. La recomanació és utilitzar Redis com a broker (o Rabbit MQ si fos necessari).
Django Yubin	DP14	Sistema d'enviament de correu amb cues i prioritats. Permet guardar els correus a base de dades i servir de buffer d'enviament.
Django modeltranslation		Farem servir preferentment Django Model Translation quan l'aplicació requereixi que la informació dins la base de dades estigui en diferents idiomes. Si fem servir django-cms com a base l'opció d'aquest és django-hvad i es farà servir directament aquest.
Django Geoposition		Solució senzilla per poder oferir un model on es desen geolocalitzacions.
GeoDjango		Framework per construir aplicacions que tinguin un component geogràfic molt important (definició d'àrees, distàncies, etc.)
Django allAuth		Integra Django amb la majoria de proveïdors de login de les xarxes socials.
Django-Rest-Framework	DP7	És l'estàndard de facto per a la creació de serveis web Rest. Permet documentar i provar els serveis.
Django-Rest-Auth	DP7	Ens proveeix d'endpoints per al registre i autenticació de Serveis Rest. És un complement



		del Django Rest Framework.
Django Redis	DP6 DP7	Gestió de catxé on es fa servir Redis com a backend de catxé
Django Compressor http://django-compressor.readthedocs.io	DP4 DP8 DP9 DP11	Comprimeix css i js i compila els arxius Less o SAAS segons sigui necessari. A producció la compilació s'ha de fer offline, perquè tot sigui 12factor.
Django Filters		Ens permet crear i definir filtres basats en paràmetres sobre la base de dades i s'integra també amb Django Rest Framework i Django Tables.
Django Tables		Presentació de la informació en format textual
Django Storages	DP8	Conjunt de <i>backends</i> d'emmagatzemament de "media" en diferents entorns (AWS S3, Google Cloud...)

19.5. Directrius de Seguretat

La seguretat de Django està activada per defecte i és necessari treballar força per tal de fer una aplicació Django insegura. Les recomanacions, per tant, estan orientades a:

[DS1] Actualitzar les versions de Django amb els darrers pegats de seguretat

[DS2] No desactivar les directives de seguretat de Django

[DS3] Utilitzar una secret key diferent per a cada aplicació i no guardar la secret key de producció al control de versions.

[DS4] Mantenir l'aplicació Django dins un entorn segur

[DS5] Fer les connexions per HTTPS

[DS6] Assegurar-se que no hi ha l'opció de DEBUG activada als entorns de producció.

[DS7] Estar al dia de les versions de seguretat dels paquets utilitzats

Per la resta les recomanacions de seguretat dependran tant de l'aplicació com d'allò que es vol protegir:

[DS8] Control del tipus de password i la seva caducitat

[DS9] Sistema d'autenticació de doble factor



[DS10] Gestió d'intents fallits de login

[DS11] Gestió de "media" privats

19.5.1. Implementacions

Eina	REF	Observacions (Descripció / Casos d'ús / Alternatives)
django-guardian		Control de permisos per objecte
Safety https://pyup.io/safety/	DS1, DS7	Check de seguretat amb opció de subscripció
django-two-factor-auth	DS9	Sistema client de doble autenticació

19.6. Directrius d'Instrumentació

[DN1] Health check. Les aplicacions que desenvolupem amb Django haurien d'exposar una url de *health check* de manera que els sistemes de monitorització puguin determinar si l'aplicació està funcionant adequadament.

Proposem una url estàndard: /health/

Aquest check de salut ha de comprovar l'estat bàsic de tots els components imprescindibles per l'operació normal: bases de dades, etc.

[DN2] Gestió d'errors. Els errors no previstos s'han de registrar i enviar de manera que puguin gestionar-se i evitar rebre milions d'e-mails d'un mateix problema depenent de la quantitat de visites que tingui un lloc web.

[DN3] Logs. L'aplicació ha d'exposar traces del seu funcionament mitjançant els logs. L'aplicació tindrà diferents nivells de logs configurats de manera que en explotació es pugui decidir quin nivell s'activa.

19.6.1. Implementacions

Eina	REF	Observacions (Descripció / Casos d'ús / Alternatives)
django-health-check	DN1	Checks extensibles amb opcions per defecte comuns
Sentry	DN2	Sistema per rebre i gestionar errors dels aplicatius

19.7. Directrius de QA (Desenvolupament)

Encara que és impossible demostrar l'absència d'errors, les bones pràctiques de qualitat de codi i control ens permeten tenir una major seguretat a l'hora de fer canvis i demostrar la idoneïtat del programa per a les tasques que ha de realitzar.

[DQ1] Unit tests. Es faran servir tests unitaris per validar les regles de negoci i les APIs pròpies i de tercers.



[DQ2] Format del codi. El codi ha de complir amb la norma PEP8 i és convenient passar un validador addicional per caçar els errors més comuns.

[DQ3] Rendiment. És convenient comprovar les queries que s'executen a la base de dades i temps de creació de les pàgines.

19.7.1. Implementacions

Eina	REF	Observacions (Descripció / Casos d'ús / Alternatives)
Unittest de Django o PyTest	DQ1	Tests Unitaris
Django Toolbar	DQ3	Permet veure les queries que es fan per generar una pàgina web i altra informació
Flake8	DQ1	Validador de PEP-8 i anàlisi de codi
Pylint	DQ1	Validador de PEP-8 i anàlisi de codi
Django Silk https://github.com/django-silk/silk	DQ1	Profiler, per quan tota la resta falla

19.8. Directrius de Documentació

Distingim dos tipus de documentació: la documentació del codi i la documentació de l'aplicatiu o per l'usuari en el cas del desenvolupament d'una llibreria o API.

Encara que Python és un llenguatge molt clar, convé documentar molt bé el codi, de manera que puguem fer ús de les capacitats dels editors moderns de mostrar-nos la documentació associada a una llibreria, classe o funció. La documentació seguirà les normes del PEP-8 de Python.

[DD1] Documentació d'aplicació. Per a documentar un aplicatiu o llibreria farem servir fonamentalment Restructured Text i la utilitat Sphinx. Restructured Text té l'avantatge de poder versionar la documentació com ho fem amb el codi, i utilitzar Sphinx per a la construcció de la documentació ens proporciona un entorn robust i amigable per consultar aquesta documentació.

[DD2] Documentació APIs. En el cas de les APIs convé documentar la seva utilització d'una manera que ens permeti testejar contra l'entorn la utilització de l'API.

[DD3] Documentació Llicències. Convé que els desenvolupadors coneguin i documentin la llicència de les aplicacions de tercers que empren, de manera que es pugui assegurar que és compatible amb l'ús i distribució que es vol fer de l'aplicació i el seu codi.

[DD4] Documentació de Desplegament. És necessari que es documentin els passos i les configuracions necessàries per tal de desplegar una aplicació. Els programadors proporcionaran la informació completa abans del desplegament: configuracions de serveis



d'analítiques, mapes, captchas, connexions API, base de dades, etc. Aquesta informació hauria d'estar al propi repositori dins un fitxer README o INSTALL i hauria de mantenir-se al llarg del cicle de vida del projecte.

19.8.1. Implementacions

Eina	REF	Observacions (Descripció / Casos d'ús / Alternatives)
Swagger http://swagger.io/	DD2	Eina de documentació REST multiplataforma i multi-llenguatge
Django-Rest-Framework <i>Built-in</i> (CoreAPI)	DD2	Documentació lligada a Django Rest Framework
Restructured Text http://docutils.sourceforge.net/rst.html	DD1	Llenguatges de documentació
Sphinx http://www.sphinx-doc.org/en/stable/	DD1	Framework per a crear documentació d'aplicatius
Read The Docs https://readthedocs.org/	DD1	Lloc on es pot publicar la documentació generada amb Sphinx.
Python Packages License Check https://github.com/briandailey/python-packages-license-check/blob/master/check.py	DD3	Si s'empra en un entorn <i>Virtualenv</i> , permet validar de manera automàtica les llicències dels paquets i aplicacions emprats per un projecte.



20. ANNEX 8: DRUPAL

20.1. Guies desenvolupament Drupal

20.1.1. Nomenclatura paquets PHP Ajuntament

Estàndards de nomenclatura mòduls, profiles i themes ajuntament.

El types associats al projectes Ajuntament són els següents:

"type": "ajbcn-drupal-profile",

"type": "ajbcn-drupal-module",

"type": "ajbcn-drupal-theme",

i els noms de projecte han de ser del tipus

"name": "ajbcn/NOM_PROJECTE"

Un Exemple de composer.json:

```
{
  "name": "ajbcn/bcn_social",
  "type": "ajbcn-drupal-module",
  "description": "Mòdul accessible per a la compartició a xarxes socials",
  "authors": [
    {
      "name": "Canals digitals",
      "email": "dti@dtibcn.cat"
    }
  ],
  "require": {
    "ajbcn/bcn_cms_stats": "*"
  }
}
```

La dependència amb el mòdul bcn_cms_stats també s'ha de posar al fitxer info.yml del projecte:

```
dependencies:
  - bcn_cms_stats:bcn_cms_stats
```



Si el mòdul té submòduls, aquesta dependència només s'ha de posar al mòdul pare (sempre que els submòduls ja tinguin especificada la dependència amb el mòdul pare).

20.1.2. Rutes i menús d'administració

Les rutes i els menús de configuració o administració dels projectes haurien de seguir aquesta estructura:

Estructura de les rutes (fitxer XXX.routing.yml)

- Tots els projectes han de preveure que l'arrel de configuració no estigui definida, per tant, és obligatori:

```
system.admin_config_bcn:  
  path: '/admin/config/bcn'  
  defaults:  
    _controller:  
      '\Drupal\system\Controller\SystemController::systemAdminMenuBlockPage'  
    _title: 'BCN'  
  requirements:  
    _permission: 'access administration pages'
```

- El formulari de configuració s'hauria de definir, doncs, a partir d'aquesta ruta arrel:

```
bcn_XXX.form:  
  path: '/admin/config/bcn/bcn_XXX'  
  defaults:  
    _form: 'Drupal\bcn_XXX\Form\BcnXXXForm'  
    _title: 'BCN XXX settings'  
  requirements:  
    _permission: 'access administration pages'
```

Estructura dels menús (fitxer XXX.links.menu.yml)

- Tots els projectes han de preveure que l'arrel de configuració no estigui definida, per tant, és obligatori:



```
system.admin_config_bcn:  
  title: 'BCN'  
  route_name: system.admin_config_bcn  
  parent: system.admin_config  
  description: 'BCN Modules.'  
  weight: -100
```

- Formulari de configuració o altres pàgines d'administració:

```
bcn_XXX.form:  
  title: 'BCN XXX'  
  description: 'Configure BCN XXX.'  
  route_name: bcn_XXX.form  
  parent: 'system.admin_config_bcn'
```

20.1.3. Guia estil codi PHP a Drupal

- Utilitzar PHPCodeSniffer amb els sniffs de la comunitat drupal que trobarem a <https://www.drupal.org/project/coder>
- Utilitzar extensió Editorconfig del nostre IDE o editor de text preferit. Si ens baixem el drupal, a l'arrel trobarem el fitxer .editorconfig que ens configura correctament els tabulats i espais dels nostres fitxers.
- A les plantilles twig evitem els comentaris HTML de l'estil `<!-- COMENTARI -->` i els posarem tots en format twig `{# COMENTARI #}`
- Per accedir als formularis administratius el permís més adequat és "administer site configurations" en comptes de "access administration pages".
- Quan cridem a la funció "t" dins d'una classe de Drupal (Controlador, Formulari, etc) hem de cridar a `$this->t('Translate me')` en comptes de cridar directament amb `t('Translate me')`. Si no ho tenim disponible a la nostra classe, podem afegir-hi la instrucció `use StringTranslationTrait;`
- S'ha de capturar correctament les `Exception` a totes les peticions amb Guzzle i s'ha de fer logging de tots els possibles problemes:

```
logginguzzleHttpException;  
use GuzzleHttp\Exception\ConnectException;  
use GuzzleHttp\Exception\RequestException;  
use GuzzleHttp\Exception\ClientException;  
  
/**  
 * Sends JSON export information to server. */
```



```
*
* @param array $jsonArray
* All export information.
* @param array $urlHost
* URL of CMS Stats web stats service without trailing slash.
*
* @return array
* Server response.
*/
private function sendJson($jsonArray, $urlHost =
BcnManager::BCN_CMS_STATS_SERVER_URL) {
    $failMessage = 'Fail: ';
    $url = $urlHost . '/bcn-cms-stats-master-api/get-notify';
    try {
        $options = [
            'headers' => ['Content-Type' => 'application/json'],
            'json' => $jsonArray,
            'timeout' => BcnCmsStatsManager::BCN_CMS_STATS_TIMEOUT,
        ];
        $response = $this->httpClient->post($url, $options);
        $response_code = $response->getStatusCode();
        if ($response_code != 200) {
            $failMessage .= $response_code;
            \Drupal::logger('bcn_cms_stats')->error('BCN CMS Stats Master send FAILED: '
. $url . ' code: ' . $response_code);
        }
        else {
            // Request OK, return updated html.
            \Drupal::logger('bcn_cms_stats')->notice('BCN CMS Stats Master send OK: '
. $url . ' code: ' . $response_code);
            return Json::decode($response->getBody()->getContents());
        }
    }
    catch (Exception | ConnectException | RequestException | ClientException $e) {
        $failMessage .= $e->getMessage();
        \Drupal::logger('bcn_cms_stats')->error('BCN CMS Stats Master send FAILED: '
. $url . ' code: ' . $e->getMessage());
    }
    $failResponse = [
        'result' => 'KO: ' . $failMessage,
    ];
    return $failResponse;
}
```

- No podem tenir una classe on tenim un únic camp que en realitat és un array associatiu que conté dins seu tots els camps de la classe. La gràcia de l'orientació a objectes es tenir N camps. Exemple:



```
class news_ok() {  
  protected $id;  
  protected $title;  
  protected $description;  
}  
  
class news_ko() {  
  protected $news;  
}
```

- A dins d'una classe, els noms de funcions i les variables han d'estar camelitzats:

```
class example() {  
  // KO.  
  protected $news_list;  
  // OK.  
  protected $newsList;  
  
  // KO.  
  public function get_range_cache_time() {}  
  // OK.  
  public function getRangeCacheTime(){  
}  
}
```

- Cal utilitzar la notació curta pels arrays ja que fa que el codi sigui més llegible: https://www.drupal.org/project/coding_standards/issues/2135291
- A dins del fitxer de configuració YAML no cal posar el prefix inicial "bcn_xxxx" donat que el nom "bcn_xxxx" ja el porta el nom del fitxer i per tant no cal complicar la jerarquia amb un nivell addicional
- Totes les peticions remotes les farem a dins d'una estructura try/catch per tenir en compte els possibles errors de xarxa i evitar pantalles en blanc.
- Fer servir la **injecció de dependència** pels nostres serveis sempre que sigui possible per evitar crides estàtiques a mètodes de classes com per exemple Drupal::config() o Drupal::service(). Consultar els possibles serveis de Drupal a core.services.yml:

```
services:  
  bcn_noticies.utils:  
    class: Drupal\bcn_noticies\BcnNoticiesUtils  
    arguments: ['@config.factory', '@entity_type.manager',  
 '@date.formatter', '@language_manager']
```



```
bcn_noticies.api:  
  class: Drupal\bcn_noticies\BcnNoticiesApi  
  arguments: ['@config.factory', '@language_manager', '@http_client',  
 '@bcn_noticies.utils']
```

- En els formularis de configuració i en els controladors la **injecció de dependència** es fa a través de la funció "create" (això ho permeten fer totes les classes que implementen la interfície **ContainerInjectionInterface**):

```
use Symfony\Component\DependencyInjection\ContainerInterface;  
  
class NoticiasFilterForm extends ConfigFormBase {  
  /**  
   * Configuration object.  
   *  
   * @var \Drupal\Core\Config\ConfigFactory  
   */  
  protected $config;  
  
  /**  
   * Configuration object.  
   *  
   * @var \Drupal\Core\Utility\LinkGenerator  
   */  
  protected $linkGenerator;  
  
  /**  
   * {@inheritdoc}  
   */  
  public function __construct(ConfigFactory $configFactory, LinkGenerator  
  $linkGenerator) {  
    $this->config = $configFactory->get('bcn_noticies.config');  
    $this->linkGenerator = $linkGenerator;  
  }  
  
  /**  
   * {@inheritdoc}  
   */  
  public static function create(ContainerInterface $container) {  
    return new static(  
      // Load the services required to construct this class.  
      $container->get('config.factory'),  
      $container->get('link_generator')  
    );  
  }  
}
```



- En els els plugins (per exemple els Blocks) la injecció de dependència es fa també a través de la funció "create" però implementen la interfície **ContainerFactoryPluginInterface** en comptes de l'interfície **ContainerInjectionInterface**. Aquesta interfície fa que tinguin tres paràmetres fixes davant:

```
use Symfony\Component\DependencyInjection\ContainerInterface;

class BcnNoticiesBlock extends BlockBase implements
ContainerFactoryPluginInterface {

    /**
     * Configuration object.
     *
     * @var \Drupal\Core\Config\ConfigFactory
     */
    protected $config;

    /**
     * Utils service.
     *
     * @var \Drupal\bcn_noticies\BcnNoticiesApi
     */
    protected $noticiesApi;

    /**
     * Url utils service.
     *
     * @var \Drupal\bcn_noticies\BcnNoticiesUrlUtils
     */
    protected $noticiesUrlUtils;

    /**
     * Constructs a new BcnNoticiesBlock object.
     *
     * @param array $configuration
     * @param string $plugin_id
     * @param mixed $plugin_definition
     * @param \Drupal\Core\Config\ConfigFactory $configFactory
     * Configuration factory.
     * @param \Drupal\bcn_noticies\BcnNoticiesApi $noticiesApi
     * Bcn Noticies API.
     * @param \Drupal\bcn_noticies\BcnNoticiesUrlUtils $noticiesUrlUtils
     * Bcn Noticies Url Utils.
     */
    public function __construct(array $configuration, $plugin_id,
    $plugin_definition, ConfigFactory $configFactory, BcnNoticiesApi
    $noticiesApi, BcnNoticiesUrlUtils $noticiesUrlUtils) {
```



```
$this->config = $configFactory->get('bcn_noticies.config');
$this->noticiesApi = $noticiesApi;
$this->noticiesUrlUtils = $noticiesUrlUtils;
}

/**
 * {@inheritdoc}
 */
public static function create(ContainerInterface $container, array
$configuration, $plugin_id, $plugin_definition) {
    return new static(
        $configuration,
        $plugin_id,
        $plugin_definition,
        $container->get('config.factory'),
        $container->get('bcn_noticies.api'),
        $container->get('bcn_noticies.urlutils')
    );
}
}
```

- Algunes injeccions de dependència necessiten de Traits com el servei de traducció (la mítica funció t). No fa falta crear el camp stringTranslation perquè ja la porta el Trait. El nom del servei a injectar és "string_translation":

```
use Drupal\Core\StringTranslation\StringTranslationTrait;
use Drupal\Core\StringTranslation\TranslationInterface;

/**
 * Provides auxiliar methods for BCN Noticies block.
 */
class BcnNoticiesBlockLister {
    use StringTranslationTrait;

    /**
     * Constructs a new BcnNoticiesUtils object.
     *
     * @param \Drupal\Core\StringTranslation\TranslationInterface
     * $stringTranslation
     * The string translation service.
     */
    public function __construct(TranslationInterface $stringTranslation) {
        $this->stringTranslation = $stringTranslation;
    }
}
```



Consideracions de seguretat al desenvolupar Drupal

Cal filtrar sempre tots els textos que imprimim al navegador i els paràmetres que ens arriben per GET o per POST. Així podem evitar injeccions de SQL i atacs de XSS (Cross Site Scripting). A continuació us mostrem funcions per Drupal 8/9 i Drupal 7 que us permetran filtrar dades en vista a la seguretat del lloc web.

IMPORTANT: Abans de passar el filtre de HTML::escape (D8) o de check_plain (D7) cal passar el filtre de XSS. L'ordre és molt important.

```
use Drupal\Component\Utility\Xss;
use Drupal\Component\Utility\Html;

/**
 * Filtre de seguretat.
 *
 * @param mixed $value
 *   Valor d'entrada.
 *
 * @return mixed
 *   Valor sanejat.
 */
public function securityFilter($value) {
    $value = Xss::filter($value);
    $value = Html::escape($value);
    return $value;
}

/**
 * Filtre de seguretat per un array qualsevol.
 *
 * @param array $params
 *   Taula d'entrada.
 *
 * @return array
 *   Taula sanejada.
 */
public function securityFilterArray(array $params) {
    $params_out = [];
    if (!empty($params)) {
        foreach ($params as $key => $value) {
            if (!is_array($value)) {
                $params_out[$key] = $this->securityFilter($value);
            }
            else {
                $params_out[$key] = $this->securityFilterArray($value);
            }
        }
    }
}
```



```
return $params_out;  
}
```

20.1.4. Gestió de codi obsolet

Consideracions generals

- A cada subversió de Drupal 8 (8.1, 8.2, etc), es van creant funcions/classes noves i d'altres es marquen com a deprecated. Per evitar problemes en el futur (quan es vagi actualitzant el core dels drupals de l'ajuntament), hauriem de llistar aquí les que ja són deprecated per evitar fer-les servir.
- El PHPStorm ens marca les crides a funcions/classes deprecated. A més a més, les podem buscar totes amb "Code > Run Inspection by Name" i tot seguit escrivim deprecated i seleccionem el deprecated de "PHP". Perquè això funcioni, haurem de tenir configurat l'editor a mode "Plugin de Drupal" on li haurem posat el path base del Drupal.

Llistat

1- Drupal\Component\Utility\SafeMarkup és deprecated.

Ara cal fer servir Drupal\Component\Utility\Html. Exemple:

```
//SafeMarkup::checkPlain($message);  
Html::escape($message);
```

2- La funció drupal_set_message és deprecated.

Ara cal fer servir el messenger. Exemple:

```
\Drupal::messenger()->addMessage(Html::escape($message));  
\Drupal::messenger()->addError(Html::escape($message));  
\Drupal::messenger()->addWarning(Html::escape($message));  
\Drupal::messenger()->addStatus(Html::escape($message));
```

3- Drupal/Core/Entity/EntityManagerInterface.php (@entity.manager) és deprecated.

Ara cal fer servir \Drupal\Core\Entity\EntityTypeManagerInterface (@entity_type.manager).



4- La constant REQUEST_TIME és deprecated.

Ara cal fer servir la següent crida:

```
\Drupal::time()->getRequestTime();
```

5- La funció format_date és deprecated.

Ara cal fer servir la funció "format" de `\Drupal\Core\DateTime\DateFormatterInterface` (@date.formatter).

6- Obtenció de l'idioma actual

Cal fer servir la funció "getCurrentLanguage" de `\Drupal\Core\Language\LanguageManagerInterface` (@language_manager).

7- La funció Drupal::l per crear links és deprecated.

Ara cal fer servir el mètode generate del servei `\Drupal\Core\Utility\LinkGenerator`

8- Drupal\Core\Entity\Query\QueryFactory (@entity.query) és deprecated.

Use the "entity_type.manager" service to get an entity type's storage object and then call `\Drupal\Core\Entity\EntityStorageInterface::getQuery()` or `\Drupal\Core\Entity\EntityStorageInterface::getAggregateQuery()` instead. See <https://www.drupal.org/node/2849874>

9- Les funcions drupal_add_feed, drupal_add_html_head, drupal_add_html_link i drupal_add_http_header de Drupal 7 són deprecated.

Cal fer servir la propietat '#attached'. See <https://www.drupal.org/node/2160069> and <https://www.axelerant.com/resources/team-blog/drupal-8-attached-part-2>

20.1.5. Variables Entorn

Introducció

Les configuracions dependent de l'entorn han d'estar com a variable d'entorn. Així no cal editar fitxers de configuració. Tot el que sigui una configuració i canviï entre entorns s'ha de definir com a tal per tal d'evitar fixar-ho (amb un *commit*) al repositori.

Hi ha una sèrie de variables d'entorn típiques (conexió a BD etc.). La majoria de variables d'entorn al servidor ja porten el valor configurat com ara la connexió a la BD.



Implementació

La implementació de les variables d'entorn està feta emprant el paquet vlucas/phpdotenv que està requerit al composer.json dels esquelets base.

També està configurat el composer.json base per executar el fitxer load.environment.php que llegirà les variables d'entorn.

Les variables d'entorn es llegeixen de servidor i es sobreescrueixen amb l'arxiu config.env. En local es pot fer l'arxiu config.env a la mateixa carpeta del composer.json.

20.1.6. Sincronització de configuració(Config Ignore, Config Split, etc)

IMPORTANT: Per norma general, fer servir només Config Ignore i la variable config_exclude_modules. Només es permet Config split en casos extremadament complexes. Perquè tot això funcioni bé, hem de fer servir Drush 10 o superior.

NORMATIVA BLOCS: Cal evitar el màxim possible l'ús de Blocs de contingut ja que, si els fem servir, quan despleguem canvis a altres entorns els haurem de col·locar a la seva regió del tema de forma manual. És per això que es recomana fer servir Plugins de bloc (BlockBase) i que aquests s'insereixin directament a les plantilles Twig (a través de les funcions del mòdul [Twig Tweak](#)). Llegir l'apartat de Config Ignore per a més detalls.

Consideracions inicials

Sempre que sigui possible, es recomana fer servir el mòdul Config Ignore i la variable de configuració del core de Drupal config_exclude_modules en comptes de fer servir el mòdul Config split.

El mòdul Config split només ens seria útil si es volen tenir configuracions comunes a dos entorns concrets. Aleshores, faríem que un split concret estigués actiu als dos entorns corresponents. Altrament, amb les dues opcions presentades anteriorment, en tindríem prou perquè ja ens permeten definir configuracions diferents als diversos entorns.

Opcions complementàries preferibles a les equivalents del Config split:

1. Tenir mòduls exclusius per entorn local (Drupal core):



Des la versió 8.8 de Drupal, podem configurar la variable `config_exclude_modules` al fitxer `settings.php` per ignorar mòduls sencers al fer `drush cex/cim`. Per més detalls, clicar [aquí](#).

```
$settings['config_exclude_modules'] = ['devel', 'stage_file_proxy'];
```

IMPORTANT: Perquè aquesta variable funcioni necessitem Drush 10 o superior.

MÒDULS D'EXEMPLE: `devel`, `stage_file_proxy`, etc.

2. Configuració que volem que pugui ser diferent a tots els entorns (Config Ignore):

Cal instal·lar el mòdul [Config Ignore](#). Ens pot ser útil per configuracions de nom de site, correu electrònic del site, codis GTM, etc.

1. Anem a `admin/config/development/configuration/ignore`
2. Afegim les configuracions que volem ignorar:

```
system.logging  
system.performance  
block.block.*
```

3. Guardem els canvis i esborrem la caché

IMPORTANT: Perquè aquest mòdul funcioni necessitem Drush 10 o superior. Només s'ignora la configuració en el moment d'importar-la. Quan l'exportem, no es té en compte la configuració d'aquest mòdul.

CONFIGURACIONS D'EXEMPLE:

- Fitxer `system.logging`: nivell d'impressió d'errors, warnings, etc de PHP al frontend.
- Fitxer `system.performance`: caché + agregació de fitxers CSS i JS.
- Fitxers `block.block.*`: instàncies de bloc que s'han col·locat a una regió del tema. Les instàncies poden pertànyer a dos tipus de bloc:
 - **Blocs de contingut:** tenen dependència amb el mòdul que els defineix i també amb el contingut del web (contingut del tipus entitat de bloc). *Es per això que cal evitar aquest tipus de bloc perquè podem arribar a trencar el lloc web si importem un block d'un contingut inexistent (per això ignorem els `block.block.*`). Però això vol dir que, al fer desplegaments, haurem de col·locar els blocs a la seva regió de forma manual.*
 - **Plugins de bloc (BlockBase):** tenen dependència amb el mòdul que els defineix. *Per tant, sempre que sigui possible, hem de treballar amb aquest tipus de blocs perquè no tenen cap mena de dependència amb el contingut.*



```
# Contingut del fitxer block.block.a.yml
(...)
dependencies:
  content:
    - 'block_content:basic:cb111028-7d9c-4a53-9d71-c64c64bd9eab'
  module:
    - block_content
  theme:
    - bartik
id: a
theme: stark
region: content
weight: 0
(...)

# Contingut del fitxer block.block.bcnoticies.yml
(...)
dependencies:
  module:
    - bcn_noticies
  theme:
    - bartik
id: bcnoticies
theme: stark
region: content
weight: 0
(...)
```

IMPORTANT: Els tipus de bloc es guarden en fitxers de l'estil `block_content.type.*`. Per tant, la seva sincronització continuarà funcionant de forma automàtica.

Funcionament Config Split

Avís molt important

Després de fer qualsevol canvi a la configuració dels splits de forma administrativa o d'esborrar un bloc d'una regió del tema, és obligatori una de les següents opcions:

- Esborrar el contingut dels directoris d'exportació principal i de cada split que tinguem.
- Executar la comanda `drush csex` en comptes de la comanda d'exportació del nucli de Drupal.

D'aquesta manera evitem problemes ja que mentre la comanda `drush` del mòdul Config split (`drush csex`) si que esborra els fitxers `yml` que es mouen a un split, la comanda `drush` del core (`drush cex` i `drush config:export`) la mou al split però no l'esborra del sync.



El mateix passa quan esborrem un bloc d'una regió del tema: si no executem la comanda `drush csex` no s'esborra el fitxer de configuració corresponent (tant si estar al directori `sync` com a un `split` qualsevol).

Procediment

1. Cal tenir configurat el directori `sync` al fitxer `settings.php`. El directori ha d'estar fora del `DOCROOT` (no ha de ser públic). És per això que es recomana que es posi el directori `config` com a germà del directori `web`:

```
$settings['config_sync_directory'] = '../config/sync';
```

0. A part del directori de `sync` cal crear un directori per cada `split` que volguem tenir. **Es proposa tenir un `split` per cada entorn (dev, pre, pro):**

2.1 Crear un nou `split` fent servir la interfície gràfica del mòdul:

- Anar a `admin/config/development/configuration/config-split`.
- Posar el nom corresponent. Exemple: `dev`.
- Li indicarem la ruta del directori així: `../config/dev`.
- Marcarem la casella de Activa.
- **Secció de Complete split (llista negra)** marcarem els mòduls i configuracions individuals que volem que siguin exclusives d'aquest entorn. Els fitxers `yml` corresponents ja no estaran al directori `sync` sinó al directori del `split` corresponent. Exemple: mòdul `Devel`.
- **Secció de Conditional split (llista gris)** marcarem la configuració que cal mantenir intacte al directori principal `sync` però que volem tenir diferent al nostre entorn local. Per tant, quan es faci `drush cex` no s'actualitzarà el fitxer `yml` del directori `sync` per no afectar la resta d'entorns. Exemple: nom del lloc, correu administratiu, codis `GTM`, els errors/warnings de `PHP` que es mostren per pantalla, etc.
- Guardarem els canvis.
- Seguirem els mateixos passos pels entorns de `pre` i `pro`.

- 2.2 Un cop creat, ens apuntem el nom màquina perquè cal configurar l'`split` que hem creat al fitxer `settings.local.php`:

```
//$config['config_split.config_split.NOM_MAQUINA_SPLIT']['status'] =  
TRUE;  
$config['config_split.config_split.dev']['status'] = TRUE;  
$config['config_split.config_split.pre']['status'] = FALSE;  
$config['config_split.config_split.pro']['status'] = FALSE;
```



NOTA: L'estat a TRUE indica que aquest split és actiu en aquest entorn i per tant s'importa la seva configuració. Altrament, si és FALS, la seva configuració s'ignora.

2.3 A l'entorn de PRE tindriem això al fitxer settings.local.php:

```
$config['config_split.config_split.dev']['status'] = FALSE;  
$config['config_split.config_split.pre']['status'] = TRUE;  
$config['config_split.config_split.pro']['status'] = FALSE;
```

IMPORTANT: Després de fer qualsevol canvi al fitxer settings.local.php cal esborrar la cache del Drupal perquè els canvis tinguin efecte.

0. És bona idea crear un split per cada entorn. Aleshores, en funció de cada entorn, tenim activat uns o altres splits mitjançant el settings.local.php.

Amb l'exemple emprat, si tenim el mòdul Devel actiu a l'entorn de dev, quan importem la configuració a l'entorn de pre el mòdul estarà inactiu.

0. **Es recomana fer servir sempre** les comandes drush de configuració del nucli de Drupal (aquestes ja tenen en compte les configuracions del mòdul Config split de BBDD actives segons el fitxer `settings.local.php`). Analitzem-ho:

4.1 A partir de drush 8.1.10:

```
# Exportació a l'entorn de DEV  
drush config:export -y  
# Exportació a l'entorn de DEV (només split dev)  
drush config:export dev -y  
  
# Importació a l'entorn de PRE/PRO  
drush config:import -y  
# Importació a l'entorn de DEV (només split dev)  
drush config:import dev -y
```

4.2 Abans de drush 8.1.10:



```
# Exportació a l'entorn de DEV
drush csex -y
# Exportació a l'entorn de DEV (només split dev)
drush csex dev -y

# Importació a l'entorn de PRE/PRO
drush csim -y
# Importació a l'entorn de DEV (només split dev)
drush csim dev -y
```

0. Comandes útils

```
drush config:status
```

Recomanacions

1. Abans d'importar i/o exportar configuració es recomana esborrar la caché

```
drush cr
```

2. Es recomana fer servir el mòdul Chosen per facilitar la configuració del Config Split:

```
composer require drupal/chosen
drush en chosen -y
drush chosenplugin
drush cr
```

20.1.7. Gestió redireccions per idioma arrel

Sempre s'ha de posar l'idioma en l'arrel de l'aplicació.

Si tenim una aplicació d'exemple amb la URL <https://www.domini.com/exemple/>, en aquesta URL s'hi ha d'afegir sempre l'idioma.

En cas que no s'expliciti el contrari l'idioma per defecte és el català (/ca).

Els idiomes **no** porten / final.



Per tant l'URL per defecte de l'arrel de l'aplicació exemple seria:

`https://www.domini.com/exemple/ca`

Per evitar duplicitat de pàgines s'ha de suprimir la barra final dels idiomes.

Així doncs s'han de configurar les redireccions:

`/ -> /ca`

`/ca/ -> /ca`

`/es/ -> /es`

`/en/ -> /en`

La manera recomanada de fer-ho es fent ús del mòdul transversal `bcn_redirect_home` o bé afegint un codi similar al següent al final del `.htaccess` de l'aplicació, canviant exemple per el prefix que correspongui:

```
<IfModule mod_rewrite.c>
  RewriteEngine on
  RedirectMatch "^/exemple/?$" "/exemple/ca"
  RedirectMatch "^/exemple/ca/$" "/exemple/ca"
  RedirectMatch "^/exemple/es/$" "/exemple/es"
  RedirectMatch "^/exemple/en/$" "/exemple/en"
</IfModule>
```

En cas que l'aplicació estigues a l'arrel del domini senzillament s'ha d'ometre el `/exemple`:

```
<IfModule mod_rewrite.c>
  RewriteEngine on
  RedirectMatch "^/?$" "/ca"
  RedirectMatch "^/ca/$" "/ca"
  RedirectMatch "^/es/$" "/es"
  RedirectMatch "^/en/$" "/en"
</IfModule>
```

En cas que el català no sigui l'idioma per defecte senzillament canviar el primer `RedirectMatch` perquè vagi a l'idioma corresponent.

20.2. Entorn local. DDEV.



L'eina que es recomana per treballar en local és el DDEV. Aquest és un entorn de desenvolupament local per a Drupal, Wordpress, etc que és similar a DrupalVM però que funciona amb Dockers i per tant no consumeix tants recursos. Els tests amb PHPUnit també funcionen bé. Actualment, és l'eina oficial recomanda per la comunitat de drupal.org.

Amb aquesta eina no cal que tinguem gaires coneixements de Docker perquè ho podem fer tot a través de la comanda ddev. De fet, podem agafar una web qualsevol i dockeritzar-la amb `ddev config` (això crea el directori ocult `.ddev` on entre altres coses hi ha el `docker-compose.yml`). Un cop fet, si tenim una BBDD per importar perquè estem muntant una web ja existent, només haurem de fer servir la comanda `ddev import-db` tal i com s'explica més endavant.

20.2.1. Instal·lació

Instal·lació ddev (macOS)

```
brew tap drud/ddev && brew install ddev
```

Instal·lació ddev (Linux)

```
curl -LO  
https://raw.githubusercontent.com/drud/ddev/master/scripts/install_ddev.sh  
&& bash install_ddev.sh
```

20.2.2. Montar entorn nova web amb ddev

ATENCIÓ: Executar el composer dins del Docker és un procés més lent que fent-ho fora a la màquina host.

ATENCIÓ: Drupal 9 necessita ddev 1.16 o superior.

Des de dins de la màquina Docker (més lent)

Instal·lació d'un nou Drupal 9

```
mkdir my-drupal9-site  
cd my-drupal9-site  
ddev config --project-type=drupal9 --docroot=web --create-docroot --  
composer-version=2  
ddev start  
ddev composer create "drupal/recommended-project"
```



```
ddev composer require drush/drush  
ddev launch
```

Si és una web existent i tenim accés al repositori

```
git clone https://github.com/example/example-site  
cd example-site  
ddev composer install  
ddev launch
```

Des de fora de la màquina Docker (més ràpid)

```
# Instal·lació drupal versió estable (última o específica)  
composer create-project drupal/recommended-project --no-interaction  
PROJECTNAME  
composer create-project drupal/recommended-project:9.0 --no-interaction  
PROJECTNAME  
  
# Si volem fer tests haurem d'instal·lar el paquet core-dev (veure pàgina  
wiki tests amb amb DDEV)  
  
# Inicialització ddev per el drupal que acabem d'instal·lar.  
cd PROJECTNAME  
# [OPCIO 1] No ens demana cap opció  
ddev config --docroot web --project-type drupal9 --composer-version=2  
# [OPCIO 2] Ens va demanant les opcions  
ddev config  
  
# Iniciem drupal i l'instal·lem amb una comanda  
ddev start  
ddev drush site-install --account-name=admin --account-pass=my-password  
  
# Connectar-nos al drupal del container  
ddev ssh  
  
# Altres comandes  
ddev exec pwd  
ddev stop
```

20.2.3. Importació de BBDD (per a webs existents)

Si ja hi ha base de dades, abans d'importar-la aquesta comanda l'esborra abans d'importar la que li indiquem.

```
ddev import-db --src=dumpfile.sql
```



Si volem exportar una BBDD d'un entorn DDEV (3 alternatives).

```
ddev export-db > dumpfile.sql.gz  
ddev export-db --gzip=false > dumpfile.sql  
ddev exec drush sql-dump > dumpfile.sql
```

Si volem exportar una BBDD en un entorn PRODUCTIU on hi ha BBDD master i esclaves i tenen GTIDs (IDs per transaccions), podem necessitar fer això:

```
drush sql-dump --extra="--set-gtid-purged=OFF --no-tablespaces" >  
EXPORT.sql
```

20.2.4. Dades importants

- Editar fitxer `.ddev/config.yml` per canviar el port de la web (per defecte és 80). **Si volem tenir actives diverses webs al mateix temps, a cada una li haurem de posar un port diferent.**
- Podem aturar el servei apache de Mac OS amb `sudo apachectl stop`
- El `docker-compose.yml` està dins el directori `.ddev`
- La comanda `ddev describe` ens imprimirà tota la info i les URL del nostre site (web, phpmyadmin, ...)
- Si al fer `ddev start` falla per algun motiu, tornem a executar la mateixa comanda un altre cop
- Al actualitzar el core o mòduls, podria ser necessari reiniciar servei i després `drush cr`
- Si volem fer servir les nostres claus SSH al container només hem d'indicar-li el directori amb `ddev auth ssh -d ~/.ssh/`

20.2.5. Comandes útils

```
docker ps -a  
ddev ssh  
ddev stop  
ddev list  
ddev delete -O PROJECTNAME  
ddev logs  
ddev logs -s db  
ddev xdebug on  
ddev xdebug off
```

És molt important que abans d'esborrar els fitxers d'una web cridem a la comanda `ddev delete -O PROJECTNAME`.

20.2.6. Migració DrupalVM/Acquia Dev Desktop a DDEV

1. Arrancar la màquina antiga i fer un backup de la BBDD del projecte amb drush



```
drush sql-dump > vm.sql
```

0. Copiar la carpeta "drupal" del projecte DrupalVM al directori de projectes DDEV. Si és Drupal 8 contindrà el drupal dins de la carpeta "web"

0. Inicialitzem DDEV (dockeritzem el projecte)

```
cd PROJECTNAME
```

```
ddev config --docroot web --project-name PROJECTNAME --project-type drupal9
```

0. Arranquem el projecte

```
ddev start
```

0. Importem la BBDD que ja teniem

```
ddev import-db --src=vm.sql
```

0. Llistem les URL del nostre lloc web

```
ddev describe
```

0. Posem la URL al navegador i ja podem començar a treballar

1. Si fa falta, haurem d'actualitzar els fitxer de configuració de PHPUnit



21. ANNEX 9: INFORMACIÓ AMPLIADA QUE ES POSA A DISPOSICIÓ (SOTA DEMANDA)

L'institut municipal d'informàtica posa a disposició del licitador la següent documentació, que serà entregada sota demanda individual, donat que per la seva extensió i en ocasions per raons de confidencialitat no s'ha adjuntat dins el plec de prescripcions tècniques:

- **Inventari de webs CMS:** Llistat dels webs CMS actualment desplegats, detallant la URL de publicació a internet, la talla (estàndard/estratègic/desenvolupament), el frontal de publicació a internet, i la seva ubicació dins l'arquitectura (clúster o dedicat).
- **Inventari de Servidors dedicats:** Llistat de servidors de cada talla, juntament amb la informació de l'aplicació que conté.
- Rànquing de **visites dels webs** (visites i pàgines vistes, corresponents a un període mensual).
- **Manual del SyGox:** Manual de l'eina de gestió d'infraestructura SyGox, on es detalla la funcionalitat i es mostra captura de pantalles.
- **Repositori de documentació WIKI** complet: exportació de tot el repositori de documentació (prop de 460 pàgines de documentació), incloent els 4 repositoris de documentació objecte d'aquest contracte:
 - Arquitectura de sistemes
 - Drupal
 - Python
 - Wordpress
- Plantilla dels comitès de direcció "Plantilla_comitè_direcció_v3.1" (Ref: apartat 3.5.4.1.3 Informe Comitè de Direcció).

22. ANNEX 10: DUBTES I ACLARIMENTS

22.1. Correu electrònic de suport

Si és de l'interès dels licitadors sol·licitar informació per la presentació de l'oferta, l'IMI posarà a disposició la següent adreça de correu on els licitadors podran fer les seves consultes: de caire tècnic: **jbitlloch@bcn.cat** , i per consultes de caire administratiu la de **imi_gestio_contractacio@bcn.cat** . En l'assumpte del correu cal indicar: "**AM – hosting lamp**".

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

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/perfil/BCN_IMI/customProf).



22.2. Sessió informativa

Es convocarà una **sessió informativa** per tal d'aclarir als licitadors interessats en presentar oferta, tots els dubtes que els hi puguin sorgir. Aquesta sessió es celebrarà a partir dels 10 dies hàbils posteriors al dia següent de la data de publicació de l'anunci de licitació en el Diari Oficial de la Unió Europea (DOUE).

El lloc, el dia i l'hora d'aquesta sessió es publicarà a l'anunci de licitació en el perfil del contractant:

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

Els licitadors hauran d'enviar per escrit (per correu electrònic) els dubtes a ser tractats a la sessió informativa, amb una antelació mínima de dos dies hàbils a la data de la sessió.

Posteriorment a la sessió, es publicarà també al perfil del contractant per escrit la relació de preguntes rebudes juntament amb un resum de les respostes donades.

Aquest document ha estat emès per el Sr. Joan Bitlloch Puigvert, tècnic responsable del contracte de l'IMI, i amb el vistiplau de,

José Antonio Tórtola
Direcció de Serveis de Desenvolupament de l'IMI
(per encàrrec de funcions)