ANNEX CLAUSULAT TECNOLÒGIC

Projecte Renovation as a Service (RaaS)

REHABILITA: PLATAFORMA DIGITAL DE SUPORT A LA REHABILITACIÓ D'HABITATGES

ÍNDEX

1. CONDICIONS GENERALS DE LA PRESTACIÓ DEL SERVEI

1.1. Arquitectures i infraestructura

1.1.1. Entorns

Les plataformes tecnològiques possibles per al desenvolupament del contracte són les següents:

- J2EE
- PYTHON/DJANGO

1.1.1.1. J2EE

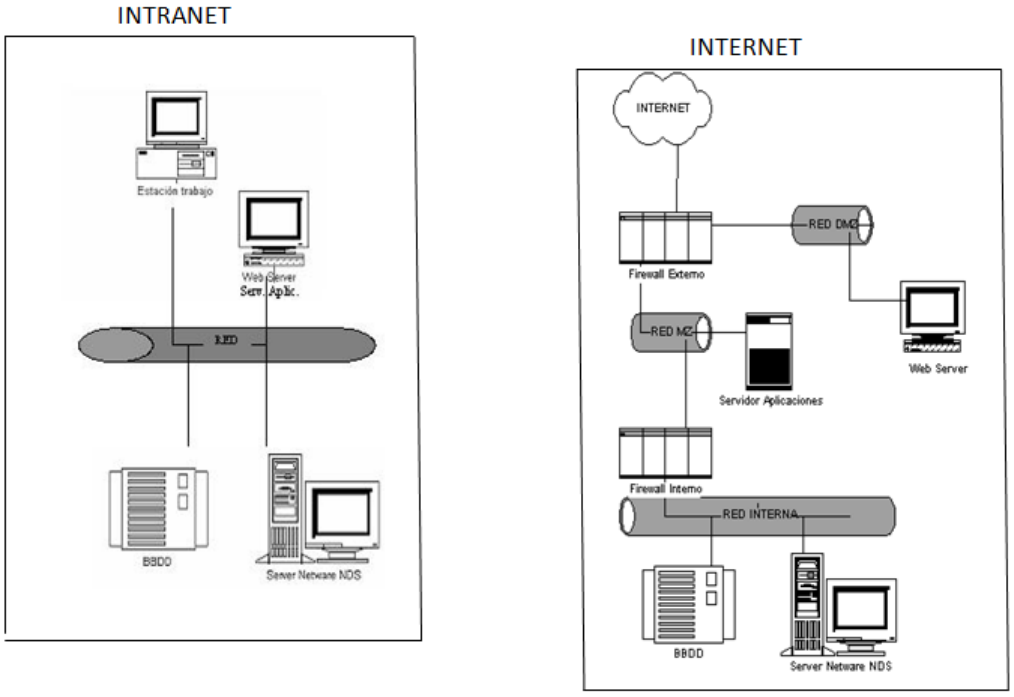
Les aplicacions desenvolupades en J2EE han de complir amb els requisits tècnics generals que es detallen al punt 10 del plec.

L'arquitectura tecnològica que en l'actualitat utilitza l'Institut Municipal Barcelona Innovació i Tecnologia (en endavant BIT) per al desenvolupament d'aplicacions J2EE es basa en els següents servidors:

Servidor Web	
Sistema operatiu	Linux SUSE 11
Servidor web	IBM HTTP Server 8.5.5
Servidor Aplicacions	
Sistema operatiu Servidor Aplicacions	Linux SUSE 11 WebSphere 8.5.5 en cluster Client WebSphere MQ 7.5
IDE	ELD(Eclipse + Tomcat/JBOSS)
Servidor OES	
Sistema operatiu	Novell Open Enterprise Server 2.0.3 (x86_64) SP3 sobre SUSE Linux 10 #1 x86_64
LDAP	eDirectory for Linux x86_64 v8.8 SP6

Servidor BBDD	
Sistema operatiu	Linux Enterprise Server 11
Servidor BBDD	Oracle 11g sobre SUSE (en curs migració a Oracle 12)

A la imatge següent es mostren els models de xarxa utilitzades per a desenvolupaments d'Internet o bé d'Intranet.



1.1.1.1.1. OpenShift (kubernetes)

La plataforma actual de desplegament a BIT és OpenShift 4.8 (o superior) basada en kubernetes.

Pel desplegament en aquest entorn cal tenir en compte que:

BIT disposa d'una plataforma pròpia de CI/CD per facilitar la construcció i el desplegament de les aplicacions. Aquesta plataforma es basa en la utilització de l'aplicació anomenada Orquestrador., que podríem definir com un Wrapper sobre l'api d'accés a kubernetes/OpenShift per tal de facilitar la construcció i el desplegament sense interacció amb els objectes de Kubernetes directament.

Aquesta aplicació s'encarrega d'iniciar la construcció de la imatge i el desplegament del contenidor a través de pipelines (jenkins) a l'entorn de BIT de forma senzilla. Al mateix temps, incorpora algunes limitacions i restriccions per estandarditzar les aplicacions que no tindríem desplegant directament sobre kubernetes.

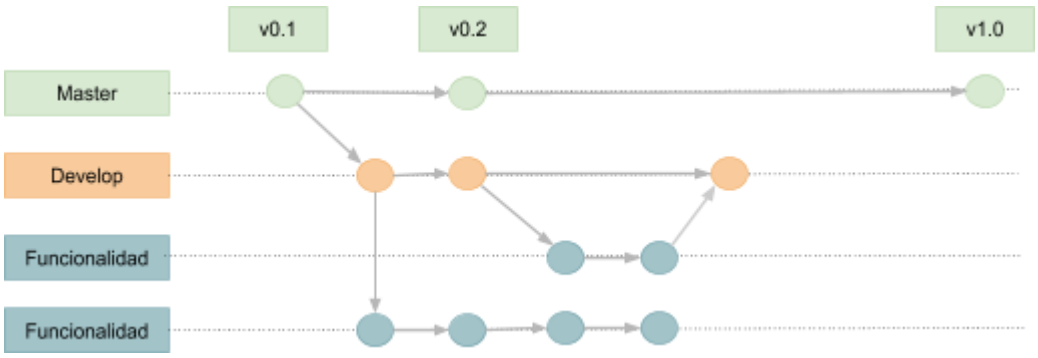
Cal tenir en compte què, com qualsevol eina, l'orquestador necessita d'un aprenentatge mínim per fer-ho servir.

La seva utilització no eximeix a l'equip de desenvolupament de tenir uns coneixements mínims de kubernetes per poder realitzar correctament la seva feina. Conceptes com: pod, replicaset, liveness i readiness, ingres (routes)... Són necessaris per realitzar un correcte desplegament i us de la plataforma.

1.1.1.1.2. Normes sobre el desenvolupament en aquesta plataforma:

Imatges base:

- Totes les imatges base fetes servir pel projecte estan restringides al conjunt d'imatges publicades al repositori de BIT. (sempre es podran demanar la inclusió d'una nova imatge a BIT si aquesta compleix amb tots els requeriments de seguretat i operacions)
- Per gestionar el codi es farà servir el gestor de codi corporatiu de l'Ajuntament, actualment Git.
- Els canvis en el codi s'hauran de pujar 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.
- Gestió del codi al repositori
    - Com a mínim es faran servir dues branques estables:
        - develop -> Contindrà el codi provat i finalitzat per desplegar a l'entorn d'integració.
        - master/main -> 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.
    - Cada nova implementació es farà en una nova branca i s'integrarà a la branca oficial quan es consideri provat i estable.
    - Esquema bàsic de funcionament:



- 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.

1.1.1.2. 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.

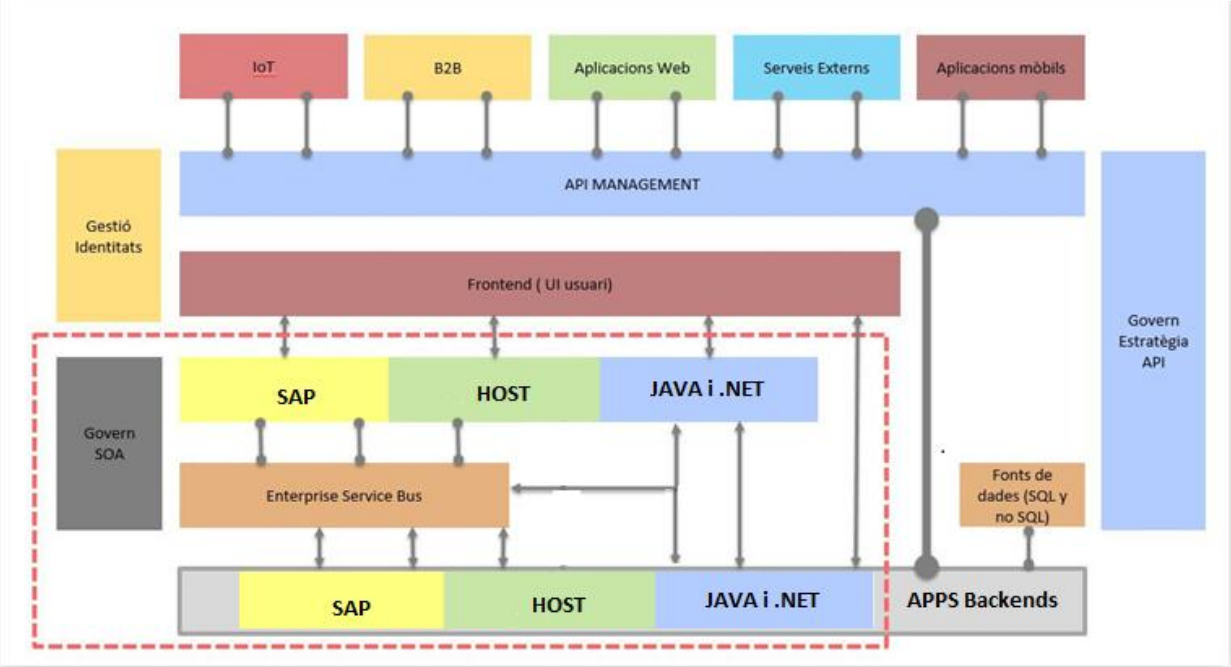
1.1.1.3. API Manager (API Connect) + BUS WebSphere Message Broker (WMB)

Històricament BIT disposa d'un bus de serveis implementat amb Websphere Message Broker. Aquest bus distribueix les crides als serveis implementats en qualsevol dels entorns principals: Host, SAP, JavaEE i .Net; des de les aplicacions i sistemes d'informació en qualsevol dels entorns clients: Host, SAP, JavaEE, .Net i Client/Servidor (estació de treball).

Es proporcionen adaptadors "nadius" que fan la funció de connexió des de cada plataforma amb les cues MQ proporcionades pel broker. També s'invoquen els serveis via transport MQ principalment.

En l'actualitat la publicació de serveis es realitza mitjançant l'API Manager d'IBM (API Connect). Aquest ha de publicar els serveis en format REST que publiquen els BackEnds.

Qualsevol integració entre plataformes que es pugui realitzar mitjançant API(s) RESTful, sempre s'ha de realitzar a través de API Manager (Ej. J2EE, Phyton, Node, etc.).



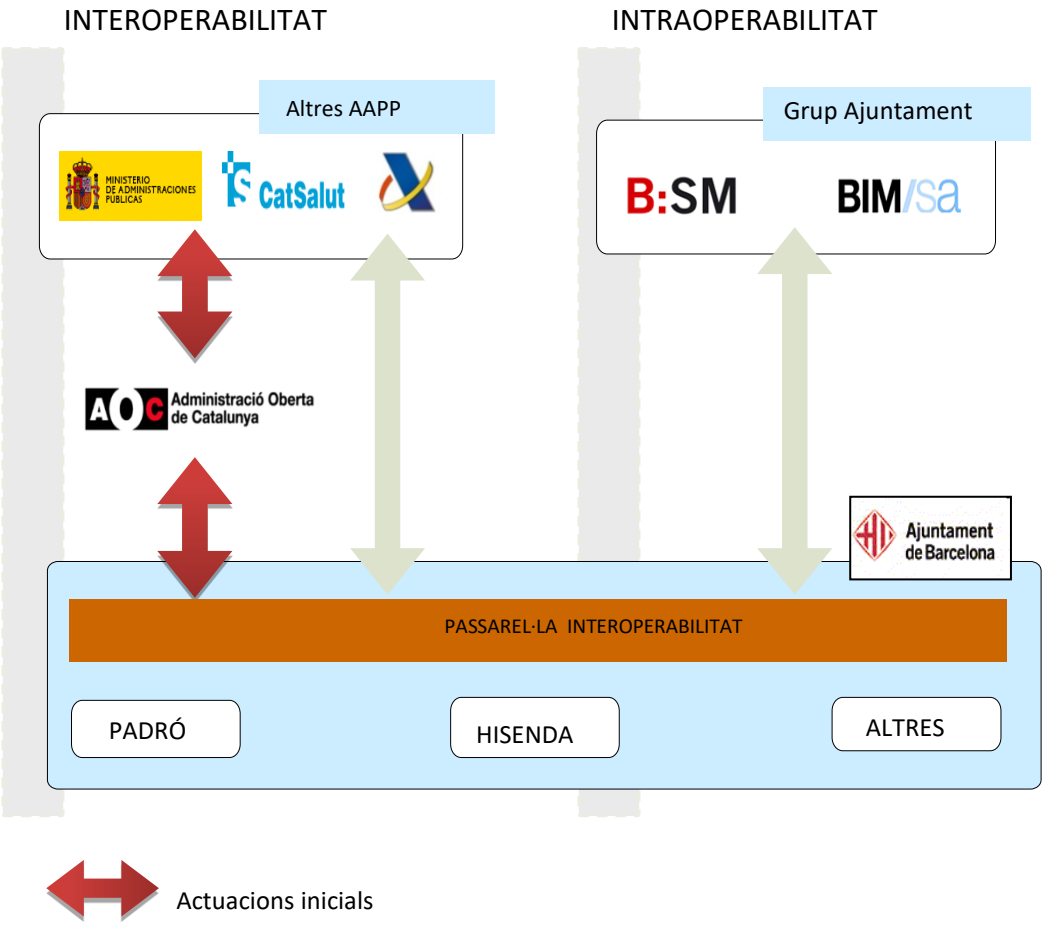
Qualsevol nova integració es farà a través de l'API Manager.

Les possibles integracions, necessàries pel sistema, existents a través del WMB es transformaran en serveis RestFul i es publicaran per l'API Manager.

1.1.1.4. Passarel·la d'Interoperabilitat de l'Ajuntament de Barcelona (PDIB)

La PDIB constitueix el suport tecnològic que garanteix la integració de dades entre el conjunt de sistemes heterogenis que donen servei als departaments de l'Ajuntament i els sistemes externs d'altres Administracions Públiques. Aquesta plataforma serveix per donar cobertura a les necessitats d'interoperabilitat de l'Ajuntament de Barcelona.

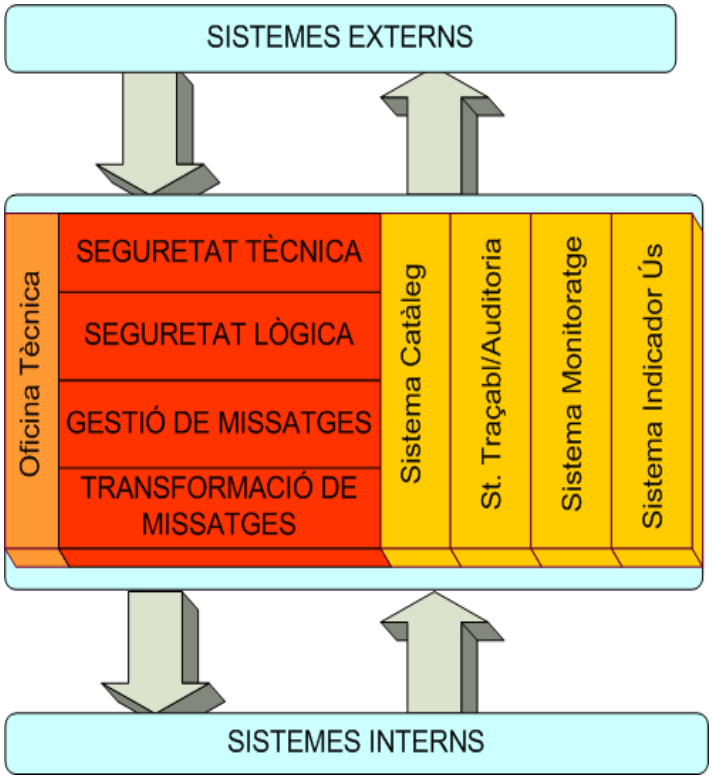
Context de la PDIB



L'accés a la PDIB es realitza a través d'una sèrie de punts d'accés o frontals WebService que es corresponen amb la natura o mode de consum del servei que es vol usar. Els punts d'accés que ofereix la PDIB consisteixen en frontals WebServices agrupats en funció de la ubicació de l'organisme que accedeix a la plataforma:

- Accessos per a organismes de la xarxa municipal.
- Accessos per a organismes externs a aquesta xarxa.

Arquitectura i subsistemes de la PDIB



- **Model d'intercanvi de dades homogeni i normalitzat entre sistemes interns i externs.**
- **Suport centralitzat per a la integració de sistemes.**
- **Simplificació del procés d'integració de nous serveis.**
- **Centralització de la informació de monitoratge, traçabilitat i indicadors d'ús.**
- **Catàleg de serveis d'intercanvi ..d'informació i SLAs**
- **Impuls organitzatiu d'una oficina d'Interoperabilitat.**

Conjuntament amb l'Oficina d'Arquitectura, es determinarà si les integracions del nou contracte es faran o no a través del PDIB.

Les possibles integracions a través del PDIB es faran de la forma que BIT determini.

1.1.2. Entorn Cloud Privat

Aquest és l'entorn gestionat per BIT. Per treballar en aquest entorn s'hauran de seguir els estàndards definits per BIT.

1.1.2.1. Estàndards de Desplegament

Se seguiran els procediments de posada en producció establerts per BIT.

1.1.2.2. Serveis transversals

BIT disposa d'un conjunt de serveis que es poden accedir des de qualsevol plataforma. Són els que anomenem Serveis transversals. L'empresa adjudicatària 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 BIT determini.

Els serveis transversals més destacats de BIT d'aplicació a aquest projecte 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).
- Plataforma d'interoperabilitat.
- Planificador de processos batch (UC4)
- Sistema de gestió de plantilles (pdfgestor)

El llistat complert 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.

BIT proporcionarà a l'empresa adjudicatària el llistat complert de serveis transversals. La utilització d'aquests serveis transversals per part de l'empresa adjudicatària ha de ser màxima.

1.1.2.3. Sistema de control de versions (GIT)

GitHub 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, GitHub 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.

BIT utilitza GitHub com a repositori de codi font de les aplicacions i serveis objectes d'aquest contracte i serà d'obligatòria utilització i administració per part de l'empresa adjudicatària.

1.1.2.4. Orquestrador

L'eina SIA es en previsió de decomisió i ser substituïda per l'eina "Orquestrador".

Aquest software es desenvolupat internament a BIT per part de l'equip d'arquitectura i abarca les necessitats de construcció i desplegament en diferents tecnologies (en creixement) a tots els entorns, recolzant-se en pipelines de Jenkins per al procediment.

Per als procediments directes a base de dades, s'utilitza la tecnologia Flyway.

Els AM son autònoms per a la construcció dels entregables i qualsevol desplegament als entorns de desenvolupament i pre-producció. Els desplegaments a l'entorn productiu han de tramitar-se mitjançant petició EasyVista.

1.1.2.5. 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 son:

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'empresa adjudicatària, 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.

1.1.2.6. Planificació de Tasques en Entorns Productius

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

Tot procés batch ha de ser cancel·lable i re-arrencable sense que requereixi cap més intervenció. També cal que s'ajusti a la finestra del batch per evitar que afecti al treball online de la persona usuària.

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 sistemes que BIT determini per aquesta tasca.

1.1.3. 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 BIT

indiquin en cada ocasió. El programari de base i de persona usuària haurà de complir l'estàndard corporatiu propi de l'Ajuntament de Barcelona, de manera que l'empresa adjudicatària estarà obligat a proveir-se d'aquest de forma prèvia.

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

En cas que la prestació del servei s'ubiqui a les instal·lacions de l'empresa adjudicatària, la connexió amb BIT 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'empresa adjudicatària.

1.1.3.1. Connexió LAN-to-LAN

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

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

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

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

A més a més, l'empresa adjudicatària 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. BIT 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, BIT 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 establir aquest circuit, BIT 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.

1.1.3.2. Software a les estacions clients

Per tal de poder executar les tasques del contracte, 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 BIT.

És responsabilitat de l'empresa adjudicatària la instal·lació, el seu manteniment, així com disposar dels equips que suportin el Software necessari a instal·lar a les màquines de l'empresa adjudicatària.

1.1.3.3. Firewall

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

Cada estació de desenvolupament només admet una connexió remota. És responsabilitat del client garantir que cada persona usuària utilitzi una màquina diferent de les que BIT els ha assignat.

Les estacions de desenvolupament estan preparades per permetre la impressió. Si es requereix algun model no reconegut, caldrà notificar-ho a BIT 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 BIT.

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

1.1.3.4. Serveis en Remot i Eines de Col·laboració

L'empresa adjudicatària haurà de garantir l'eficiència i la productivitat del seu equip treballant en remot, utilitzant les eines de col·laboració, comunicació i gestió de projectes que el BIT determini (ex: Microsoft Teams, Jira, Confluence, etc.). S'haurà d'assegurar una comunicació fluida i constant entre els membres de l'equip de l'adjudicatari i amb els interlocutors del BIT i de les àrees de negoci de l'Ajuntament, independentment de la ubicació física.

1.1.4. Components de software lliure

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

Les solucions, sistemes, processos i metodologies que es defineixin hauran d' estar alineats i 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 de persona usuària
- Ús prioritari de Programari Lliure.

- Compartició i creació de solucions de forma col·laborativa amb comunitats i altres administracions.
- Interoperabilitat
- Dades obertes
- Aplicació d'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'aplicaran les definicions de l'Open Source Iniciative (https://opensource.org/).

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

En els casos 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.

2. QUALITAT DELS SERVEIS

2.1. Pla de qualitat

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

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

- 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 de l'empresa proveïdora
    - 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'empresa adjudicatària haurà d'executar el Pla de Qualitat específic que asseguri la qualitat dels serveis oferts.

2.2. Qualitat del servei

Li correspon a l'empresa adjudicatària 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, BIT exigirà l'acompliment dels nivells de servei descrits al PPT i obliga a l'ús de la metodologia ADINET o la Metodologia AGILE Scrum@BIT en totes les tasques que executi l'empresa adjudicatària.

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, BIT 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 BIT per a la seva consideració i validació en cas que ho consideri necessari.

2.3. Auditories

BIT, 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.

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

- Periodicitat: A determinar per BIT
- 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

2.3.1. 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 BIT, sobre el grau de compliment del les empreses adjudicatàries amb els aspectes formals del servei.

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

- 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'empresa adjudicatària per a les seves pròpies activitats (controls, revisions, proves, auditories internes de l'empresa adjudicatària, 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.

2.3.2. Procediment d'Auditoria

L'auditor farà l'anàlisi que consideri necessari i requerirà a l'empresa adjudicatària tota aquella informació que consideri adient.

L'empresa adjudicatària 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'empresa adjudicatària 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'empresa adjudicatària associats a les auditories no podran ser repercutits en cap cas a BIT.

2.3.3. 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 altra 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'empresa adjudicatària haurà d'establir un Pla d'acció 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.

L'empresa adjudicatària haurà de presentar a BIT el Pla d'acció en el termini d'un mes des de la comunicació dels resultats finals de l'auditoria. Serà responsabilitat de l'empresa adjudicatària la realització de les accions en els terminis establerts en el Pla d'acció.

2.3.4. Resultats de la Revisió

BIT 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".

Al plec administratiu es detallen sancions per les "No Conformitats" no tancades.

2.4. Qualitat de Programari

El conjunt del programari objecte d'aquest plec estarà subjecte als controls de qualitat o verificació de validesa que BIT determini. En aquest sentit l'empresa adjudicatària haurà de procedir a realitzar el conjunt de proves funcionals i tècniques que BIT 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 BIT determini, obligant-se l'empresa adjudicatària a la realització i/o col·laboració en la confecció dels scripts corresponents a tal efecte.

3. ACORDS DE NIVELL DE SERVEI (ANS)

Per a la gestió i seguiment dels serveis prestats per a l'empresa adjudicatària, es defineixen una sèrie d'Acords de Nivell de Servei (ANS) que les empreses licitadores poden complementar i/o millorar. Aquests permeten monitoritzar i avaluar la qualitat, i, la gestió dels serveis a través d'indicadors que parametritzen el grau de consecució acordat per a cada servei.

Els ANS s'estructuren en funció dels diferents serveis principals definits en aquest plec:

- Servei 1: Implementació
- Servei 2: Estabilització
- Servei 3: Manteniment.

Per a cada indicador dels ANS, es definirà:

- Codi de l'Indicador: Identificador únic de l'ANS.
- Nom de l'Indicador: Descripció clara de l'aspecte del servei que es mesura.
- Descripció Detallada: Explicació del propòsit de l'indicador, com es mesura, les fonts de dades, la fórmula de càlcul (si aplica) i qualsevol aclariment necessari per a la seva correcta interpretació en el context del projecte.
- Periodicitat de Mesura: Freqüència amb la qual es calcularà i s'avaluarà l'indicador (ex: mensual, trimestral, per fita).
- Valor Objectiu/Llindar: Nivell mínim de compliment esperat per a l'indicador.
- Mecanisme de Verificació: Com el BIT verificarà el compliment de l'ANS.
- Penalització per Incompliment: Conseqüències associades a l'incompliment de l'ANS.

3.1. ANS per al Servei 1. Implementació

Els ANS per a aquest servei se centren en garantir la qualitat, el rigor i l'oportunitat en les fases inicials i transversals de definició i disseny de les solucions. Es busca assegurar que la planificació sigui sòlida, els requisits estiguin ben definits i els dissenys tècnics i funcionals siguin de la màxima qualitat i s'alineïn amb les directrius corporatives.

Codi	Nom de l'Indicador	Descripció Detallada	Periodicitat	Valor Objectiu/Llindar	Descompte factura

ANS-S1-01	Lliurament Puntual de Documentació Clau de Llançament	Percentatge de documents clau de la fase de llançament del projecte/release (Pla de Projecte, Pla de Riscos Inicial, Pla de Qualitat Específic) lliurats dins dels terminis acordats amb el BIT.	Per Fita	≥95%	3% del total de facturació de la 1a release del Servei 1
ANS-S1-02	Qualitat de la Documentació d'Anàlisi i Disseny	Percentatge de documents d'anàlisi i disseny (Especificació de Requisits, Document d'Arquitectura de Solució, Disseny Tècnic Detallat) acceptats pel BIT en la primera revisió formal o amb un màxim d'una iteració de canvis menors.	Per Release	≥90%	3% del total de facturació del Servei 1 per la Release en que succeeixi aquesta situació
ANS-S1-03	Alineament dels Dissenys amb Estàndards BIT	Nombre de No Conformitats Majors identificades en la revisió dels documents d'arquitectura i disseny tècnic respecte als estàndards i millors pràctiques i directrius del BIT.	Per Release	0 No Conformitats Majors	3% del total de facturació del Servei 1 per la Release en que succeeixi aquesta situació
ANS-S1-04	Compliment de Terminis en Fases de Consultoria/Disseny	Percentatge de fites clau de les fases de consultoria, anàlisi i disseny completades dins dels terminis establerts en el Pla de Projecte aprovat.	Per Release	≥90%	3% del total de facturació del Servei 1 per la Release en que succeeixi aquesta situació

ANS-S1-05	Traçabilitat dels requisits a la presa de decisions en les propostes de solució d'arquitectura i disseny tècnic	Valoració per part del BIT de la base de coneixement i traçabilitat documentada de la presa de decisions en les propostes de solució d'arquitectura i disseny tècnic per donar resposta a cadascuna de les funcionalitats incloses en les èpiques definides per release.	Per Release	Mitjana ≥4 (en una escala d'1 a 5)	3% del total de facturació del Servei 1 per la Release en que succeeixi aquesta situació

Els ANS per a aquest servei estan orientats a garantir la qualitat de la construcció tècnica de la solució l'eficàcia dels processos de proves i la correcta implantació en els diferents entorns, assegurant l'estabilitat i el compliment funcional.

Codi	Nom de l'Indicador	Descripció Detallada	Periodicitat	Valor Objectiu/Llindar	Descompte factura
ANS-S2-01	Cobertura de Proves Unitàries	Percentatge mínim de cobertura de codi aconseguit per les proves unitàries per a totes les classes i triggers desenvolupats o modificats.	Per Release	≥60%	2% del total de facturació del Servei 2 per la Release en que succeeixi aquesta situació
ANS-S2-02	Densitat de Defectes en UAT	Nombre de defectes de severitat alta o crítica identificats durant les Proves d'Acceptació d'Usuari (UAT) per cada punt d'història o unitat de funcionalitat equivalent lliurada.	Per Release	≤3 defectes/punt d'història	2% del total de facturació del Servei 2 per la Release en que succeeixi aquesta situació

ANS-S2-03	Compliment de Terminis de Lliurament d'Increments	Percentatge d'històries d'usuari o funcionalitats compromeses en un sprint/release que es lliuren completades (complint DoD) dins del termini del sprint/release.	Per Release	≥90%	2% del total de facturació del Servei 2 per la Release en que succeeixi aquesta situació
ANS-S2-04	Èxit dels Desplegaments a Entorns Superiors	Percentatge de desplegaments a entorns de proves superiors (Integració, UAT, Preproducció) que es completen amb èxit en el primer intent, sense necessitat de rollback o correccions urgents post-desplegament.	Mensual	≥90%	2% del total de facturació del Servei 2 per la Release en que succeeixi aquesta situació
ANS-S2-05	Estabilitat Post-Implantació	Nombre d'incidències crítiques o bloquejants originades per la nova funcionalitat desplegada, reportades durant les primeres dues setmanes posteriors a una posada en producció.	Per Release	≤2 incidències	2% del total de facturació del Servei 2 per la Release en que succeeixi aquesta situació
ANS-S2-06	Qualitat de la Documentació Tècnica i d'Usuari de la Release	Valoració per part del BIT de la completitud, claredat i precisió dels manuals d'usuari, guies d'administració i documentació tècnica actualitzada per cada release.	Per Release	Mitjana ≥4 (en una escala d'1 a 5)	2% del total de facturació del Servei 2 per la Release en que succeeixi aquesta situació

ANS-S2-07	Traçabilitat dels Requisits a les Proves	Percentatge d'històries d'usuari i criteris d'acceptació definits per a una release que compten amb una cobertura explícita i verificable per casos de prova funcionals i/o UAT documentats.	Per Release	≥90% dels criteris d'acceptació amb traçabilitat a casos de prova	2% del total de facturació del Servei 2 per la Release en que succeeixi aquesta situació

3.2. ANS per al Servei 2: Estabilització

Els ANS que aplicarien per aquest servei serien el global dels associats al punt Servei 3: Manteniment. També són d'aplicació els relatius al Servei 1 davant modificacions rellevants tractades com un projecte, o els relatius a deficiències evidents i rellevants associades a la gestió, qualitat o documentació realitzada.

3.3. ANS per al Servei 3: Manteniment

Els ANS per al servei de manteniment i evolució se centren en garantir la disponibilitat, el rendiment i la fiabilitat de la plataforma en producció, així com l'atenció eficient a les necessitats de suport i l'evolució contínua de la solució. Es classifiquen les incidències i peticions segons la seva criticitat (Urgent, Greu, Normal, Baixa), que serà definida en col·laboració amb el BIT a l'inici del servei.

3.3.1.1. Manteniment Correctiu

El càlcul dels següents ANS s'haurà de fer per petició de manteniment correctiu, incidència i suport, associat als serveis transversals de manteniment **amb periodicitat mensual** i considerant hores laborables i mes natural.

Indicador	**Descripció**	**Càlcul**	**Gravetat incidència / suport**	**ANS**	**Descompte factura**
Temps de resolució incidència i suport **(Inc TReso)**	Temps que transcorre entre la comunicació d'una incidència o suport i la resolució efectiva. No ha de superar el llindar d'hores definit	Inc Treso = Data resolució incidència/suport (*) - data d'entrada incidència/suport	urgent	Inc Treso <= 8 hores laborables	Import de les hores treballades a la incidència/ suport
			greu	Inc Treso <= 24 hores laborables	Import de les hores treballades a la incidència/ suport

Indicador	Descripció	Càlcul	Gravetat incidència / suport	ANS	Descompte factura
			normal	Inc Treso <= 40 hores laborables	Import de les hores treballades a la incidència/ suport
			baixa	Inc Treso <= 80 hores laborables	Import de les hores treballades a la incidència/ suport
Temps de tancament d'incidència i suport **(Inc tanc)**	Temps que transcorre entre la comunicació d'una incidència i suport i la resolució efectiva. No ha de superar el llindar d'hores definit, que és de 24 hores laborables addicionals sobre el llindar de Treso per a la mateixa criticitat d'aplicació/ Incidència	Inc tanc = Data resolució incidència/ suport (*) - data d'entrada incidència/suport	urgent	Inc tanc <= 32 hores laborables	200 € per incidència/ suport que incompleixi l'ANS
			greu	Inc tanc <= 48 hores laborables	200 € per incidència/ suport que incompleixi l'ANS
			normal	Inc tanc <= 64 hores laborables	200 € per incidència/ suport que incompleixi l'ANS
			baixa	Inc tanc <= 104 hores laborables	200 € per incidència/ suport que incompleixi l'ANS

Indicador	Descripció	Càlcul	Gravetat incidència / suport	ANS	Descompte factura
Incidències i suport Pending **(Inc Pen)**	Nª d'incidències i suport amb estat pending sense justificació i no acordades amb responsable del BIT	Inc Pen = nombre d'incidències/ suports amb estat pending sense justificació i no acordades amb responsable del BIT		Inc Pen=0	200 € per incidència/ suport que excedeixi l'ANS
Incidència i suport no resolta **(Inc no res)**	Incidències i suports no resolts en la data prevista Inc Tanc	Inc no res = Nº incidències/ suports que tenen activat l'ANS Inc tanc en la data del comitè i no estan resoltes			200 € per incidència/ suport que incompleixi l'ANS (**)
Tancament de problemes **(Pr tanc)**	Problema resolt i lliurat al BIT a la data compromesa.	Pr tanc = Data de lliurament (*) - Data compromesa		Pr tanc <= 0 dies laborables	3.000 € per problema que excedeixi l'ANS

3.3.1.2. Manteniment Recurrent

El càlcul dels següents ANS s'haurà de fer per cada petició de manteniment recurrent **i 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 manteniment o evolutiu recurrent i el lliurament al BIT 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 o evolutiu recurrent realitzat i lliurat al BIT 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

3.3.1.3. ANS 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
Qualitat dels documents entregats **(Qinf)**	Documents (actes, informes, valoracions i altra documentació del servei) entregats amb més d'una iteració per manca de qualitat en la seva elaboració	Qinf = nº documents entregats amb més d'una iteració per manca de qualitat	Qinf<=0	200 € per document amb més d'una iteració per manca de qualitat
Qualitat del manteniment entregat **(Qmt)**	Lliurables (correctiu, recurrent i evolutius) entregats amb més d'una iteració per manca de qualitat en la seva elaboració	Qmt = nº lliurables entregats amb més d'una iteració per manca de qualitat	Qmt<=0	200 € per lliurable amb més d'una iteració per manca de qualitat

Indicador	Descripció	Càlcul	ANS	Descompte factura
Temps de resolució de petició **(Pet Treso)**	Temps que transcorre entre la comunicació d'una petició i la seva resolució efectiva.	Pet Treso = Data resolució petició - data d'entrada petició	Pet Treso <= 5 dies laborables	200 € per petició que incompleixi l'ANS
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<=0	100 € per tiquet tancat identificat a l'eina de ticketing amb falta de qualitat

Notes Importants sobre els ANS:

- Definició Detallada: Tots els indicadors, les seves mètriques exactes, els llindars específics (valors X, Y, Z, N), els criteris de classificació de criticitat, les finestres de mesura exactes (ex: "horari laboral") i els mecanismes de càlcul seran detallats i acordats formalment entre el BIT i l'empresa adjudicatària a l'inici del contracte, i podran ser revisats i ajustats de mutu acord durant la vigència del mateix si les circumstàncies ho justifiquen.
- Eines de Suport: L'adjudicatari haurà d'utilitzar les eines de gestió de projectes, ticketing i documentació que el BIT determini (ex: Jira, Confluence) per facilitar el registre, seguiment i la generació d'informes necessaris per al càlcul dels ANS.
- Excepcions: Es podrà preveure un mecanisme per gestionar excepcions justificades al compliment dels ANS (ex: incidències causades per tercers aliens al control de l'adjudicatari, canvis d'abast no planificats amb impacte directe), que hauran de ser documentades i aprovades pel BIT.
- Millora Contínua: Els resultats dels ANS s'analitzaran periòdicament en els comitès de seguiment i s'utilitzaran com a base per identificar àrees de millora contínua en la prestació del servei i en la pròpia plataforma.

4. REQUERIMENTS ESPECÍFICS

4.1. Requisits generals

Addicionalment als requisits particulars tot procés o funcionalitat haurà de contemplar els següents requisits de caràcter general:

4.1.1. 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 una persona usuària haurà de ser menor a 4 hores.

RU4. [Obligatori] El sistema disposarà de manuals de persona usuària estructurats adequadament.

RU5. [Obligatori] El sistema ha de proporcionar missatges d'error que siguin informatius i orientats a persona usuària 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 Multidispositiu, 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).

4.1.2. Eficiència

L'empresa adjudicatària 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 BIT 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 la persona usuària 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 la persona usuària 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 la persona usuària per mantenir-se ininterrompuda, tot i que la persona usuària 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 la persona usuària perd la sensació de operar directament sobre les dades.
- 10 segons és el límit per mantenir l'atenció de la persona usuària centrada en el diàleg. Per a retards més llargs, les persones usuàries 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 les persones usuàries no saben què esperar.

RE2. [Obligatori] El sistema ha de ser capaç d'operar adequadament amb les persones usuàries 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'empresa adjudicatària 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.

4.1.3. 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 la persona usuària 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.

4.1.4. Logs d'execució dels processos batch

Tots els processos batch han d'extreure uns logs d'execució que permetin a la persona usuària 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 la persona usuària i d'ús fàcil i particular per a cada procés.

4.1.5. 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.

4.1.6. 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.

4.1.7. 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 seqüencies 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 complert de tota l'execució).

L'empresa proveïdora presentarà un pla d'execució dels processos batch que passarà a validació de BIT tenint en compte tots aquests aspectes amb la suficient antelació per la seva planificació i posada en productiu.

4.1.8. 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.

La persona usuària 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'empresa adjudicatària serà el/la responsable de la confecció dels jobplans segons indicacions del departament d'Explotació de BIT (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.

4.1.9. 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).

4.1.10. 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'empresa adjudicatària col·laborarà amb els ajusts que siguin necessaris per fer-ho possible.

La Geocodificació 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.

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).

4.1.11. 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 la persona usuària 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 bmp.
- 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.

L'empresa proveïdora serà el/la responsable de la gestió de la generació i validació dels documents i plantilles afectats per part de la persona usuària 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.

4.1.12. Assignació de rols

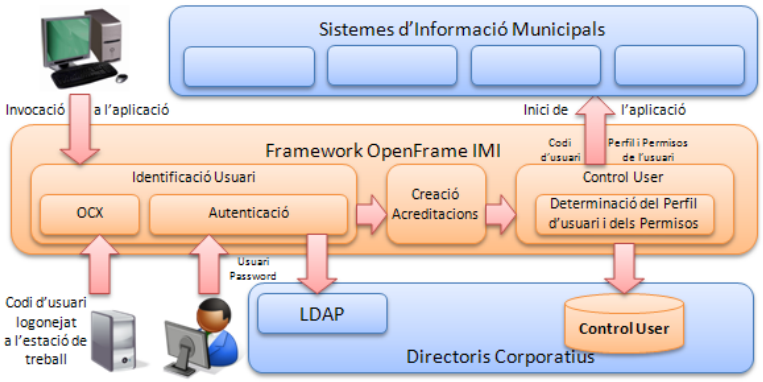
1. **Autenticació de persones usuàries**

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 de les persones usuàries, 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 BIT. Per a aplicacions .NET les funcions estan desenvolupades al NET Framework de BIT

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 de persona usuària que ja ha estat prèviament autenticat a aquesta estació de treball i utilitza aquest codi per a la identificació de la persona usuària 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 de persona usuària, cosa que provocarà que el sistema demandi aquestes dades a la persona usuària.

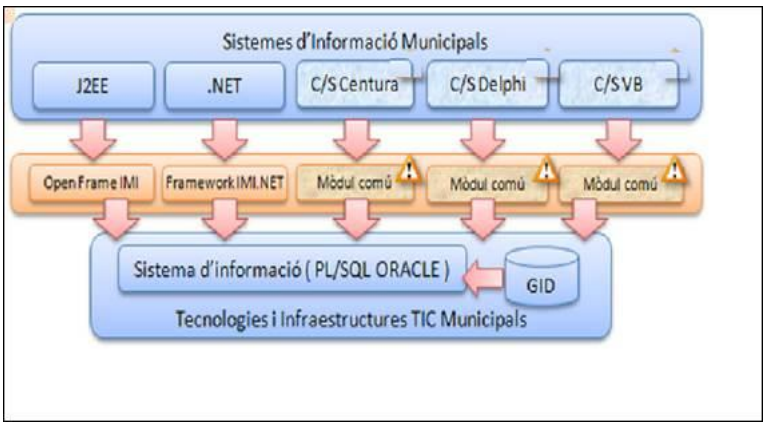
Un cop efectuada l'autenticació (per codi d'estació de treball o per persona usuària i clau d'accés informats) es procedeix a determinar el perfil i els permisos de que es disposarà a l'aplicació durant la sessió present. Per a aquesta funció s'utilitza el sistema general anomenat "Control User", i que es descriu a l'apartat Gestió de perfils i permisos de persones usuàries "CtrlUsr".



Finalment es dona control a l'aplicació informant del codi de persona usuària que hi accedeix i del perfil i permisos que ostentarà.

2. Gestió de persones usuàries i Permisos

La CtrlUsr es el sistema d'informació que permet gestionar l'autenticació i l'autorització de les persones usuàries a les aplicacions, mitjançant un catàleg d'aplicacions, una llista de funcions agrupades en perfils i aquets perfils assignats a persones usuàries. Aquest sistema d'informació, és utilitzat en totes les plataformes de desenvolupament de BIT (a excepció de Host i SAP).



4.1.13. Llistats, informes i explotació de la informació

S'hauran de configurar en les eines que BIT disposi o en el seu defecte desenvolupar tots els llistats necessaris per garantir l'operativa diària de l'Ajuntament de Barcelona. A l'inici del contracte, BIT 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 la persona usuària 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.

4.1.14. 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'empresa adjudicatària 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.

Addicionalment, 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.

4.1.15. 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 BIT 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'empresa adjudicatària 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 complert.

4.1.16. Monitorització del servei

L'empresa adjudicatària 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. BIT col·laborarà amb la persona usuària i l'empresa adjudicatària en la definició del millor cas d'ús possible.

4.1.17. Requisits tècnics visors mapes

Caldrà tenir en consideració els següents requeriments tècnics específics en relació a la visualització de mapificació de dades:

- **T1: Ús de Geocomponents (GeoBCN) per a la representació de mapes**
  El sistema ha d'usar els serveis i API GeoBCN en la seva darrera versió. BIT disposa de documentació tècnica, exemples relacionada amb l'API JS i l'API de serveis que cobreixen les necessitats del projecte en matèria de geocodificació i representació cartogràfica a partir de la cartografia oficial de l'ajuntament.
- **T2: Llibreries i llenguatge de programació del visor (Frontend/SPA)**
- El visor es desenvoluparà a partir del framework Vue.js, en la seva versió 3, i estructurant el codi a partir de Composition API. El projecte inclou les següents llibreries per a la implementació dels diferents blocs funcionals:
  - Geolocalització i mapes: GeoBCN i OpenLayers
  - VUEi18n per a la internacionalització
  - PrimeVue, per a components UI
- **T3: Llenguatge de programació de serveis i lògica de negoci (Backend)**
  El desenvolupament del backend i els serveis necessàries es podran desenvolupar amb les dues tecnologies en ús a BIT, consistents en J2EE i/o Python segons les directrius i bones pràctiques descrites en els annexes corresponents.
- **T4: Entorn DevOps (OCP) i dockerització**
  Caldrà orientar l'aplicació al funcionament en contenidors Dockers, replicant d'aquesta manera als contenidors la mateixa infraestructura productiva. Per això es partirà d'imatges preparades per BIT que s'hauran de fer servir de base per a la construcció de les imatges definitives que caldrà desplegar en la plataforma DevOps (OCP) de l'Ajuntament

- **T5: API Manager (API Connect)**
  L'API desenvolupada per l'accés a la informació s'ha de publicar i integrar amb API Manager per tal que segueixi les directives de desenvolupament actual. Aquest ha de publicar els serveis en format REST que publiquen els BackEnds. Qualsevol integració entre plataformes que es pugui realitzar mitjançant API(s) RESTful, sempre s'ha de realitzar a través de API Manager (Ej. J2EE, Python, Node, etc.).
- **T6: Multidispositiu**
  Els visors han de posseir un disseny "Responsive" i Multidispositiu, a fi de garantir l'adequada visualització a múltiples dispositius: DeskTop, Tables i Telèfons Intel·ligents.

4.2. Requisits d'arquitectura

RA1. [Obligatori] Llenguatges de programació i Frameworks

Els llenguatges "base" per programar les aplicacions a mida a l'Ajuntament de Barcelona son JavaEE i Python.

Quan el llenguatge "base" sigui JavaEE BIT disposa d'un framework propi de anomenat OpenFrameBIT i que, actualment, es troba en la versió 4. Aquest framework és d'**utilització opcional** per al desenvolupament d'aplicacions Java. Cal destacar que el framework openFrameBIT 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 del BIT **No fixen la capa de presentació**, però aposten per front-ends (SPAs Single Page Applications).

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 de 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

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.

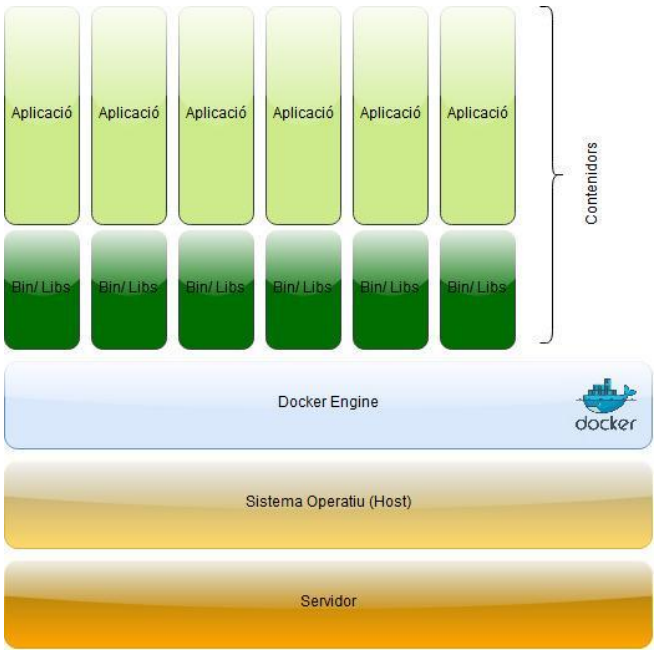
RA3. [Obligatori] Preparada per a ser Desplegada en contenidors dockers

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 BIT que s'hauran de fer servir de base per a la construcció de les imatges definitives que caldrà desplegar.

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 BIT 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

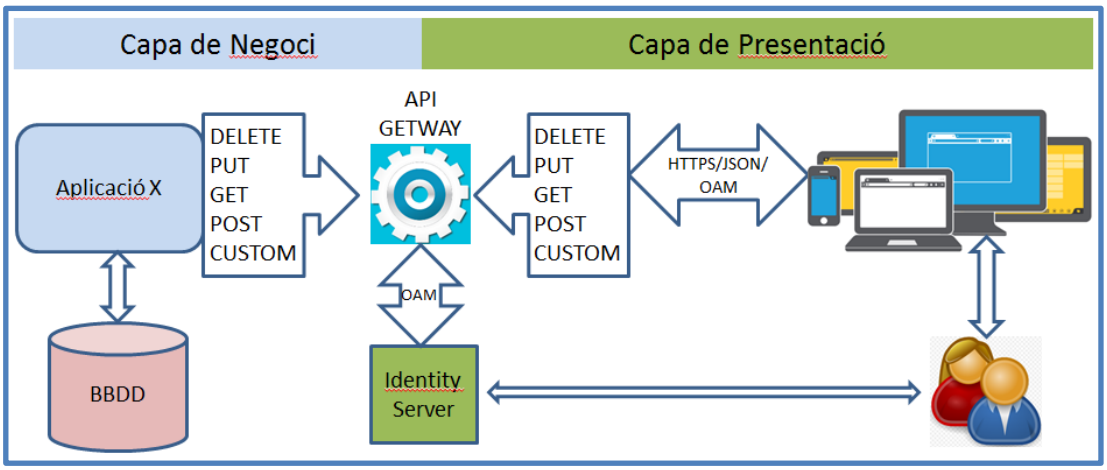
Per eficiència i sostenibilitat el sistema a construir haurà de ser modular i escalable: ha de tenir un enfocament prou transversal com per minimitzar l'impacte de la incorporació de noves funcionalitats.

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 Getway i el client(Presentació). La imatge de sota Il·lustra com interactuen AQUESTS 3 components.

Com a mínim tota aplicació tindrà 2 instal·lables: Serveis (Negoci que es publicarà a l'API Getway) i el client (Presentació).



Serveis (Negoci) – Noves aplicacions

- L'instal·lable haurà de seguir una arquitectura de "*monòlit modular*" no pas de *microserveis*. Referència
- 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 una persona usuària (nominal o de servei) per tal de poder consumir el servei.
        - Això comporta fer una autenticació amb la persona usuària 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 de les persones usuàries.
- La capa de presentació és la responsable de generar les pantalles a la persona usuària i d'atendre les seves peticions. **No ve fixada pel framework de BIT**.
- Pot estar basada en el framework estàndard per a aplicacions SPA de BIT: Arquitectura Angular + Bootstrap com framework de presentació. És responsable de generar les pantalles a la persona usuària 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 (veure l'apartat de requisits de seguretat).
- 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 BIT.

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)

RA7. [Obligatori] Estructura multi-idioma

La solució ha de ser multi-idioma. La totalitat dels camps/missatges visibles per la persona usuària 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*).

BIT 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

Addicionalment, el sistema haurà de garantir la traçabilitat de les accions de les persones usuàries sobre el mateix.

RA9. [Obligatori] Components de software lliure

BIT 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

BIT 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 BIT.
- **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 la persona usuària i on s'han de deixar instal·lades les aplicacions.

Totes les aplicacions lliurades a BIT 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 BIT 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, BIT limita les diferents tecnologies en les que es poden implementar les seves aplicacions.

Actualment BIT 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 BIT:
    - 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 instancia Corporativa, 1 únic servidor de BD per n projectes
      - BIT gestiona aquesta infraestructura

A més d'aquestes tecnologies, i/o llenguatges de programació, BIT 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 BIT.

4.3. Requisits d'informació de base i cartografia

Donat que la pràctica totalitat de l'activitat de l'Ajuntament de Barcelona està relacionada amb persones i/o amb territori, BIT disposa d'un model de dades, Model d'Informació de Base, d'ara en endavant MiB, que conté les dades bàsiques d'aquests dos grups, a més de les relacions que persones i territori mantinguin amb l'Ajuntament.

L'objectiu del MiB és aconseguir la unificació de les dades de persones i objectes territorials (parcel·les, adreces postals i locals) per evitar dades duplicades, incoherències i errors per una manca de qualitat de les dades des de les aplicacions origen.

Els diferents elements que configuraran aquest model de dades són:

- **Persones**. Conjunt de persones físiques o jurídiques que es relacionen amb l'Ajuntament, en el marc d'una relació reglada de negoci.
- **Objectes territorials**. Elements que configuren l'espai urbà, tant el públic com el privat, de la ciutat de Barcelona.
- **Negocis**. Prestació de serveis subjectes a regulació, actes administratius o fets imposables establerts per l'Ajuntament.

Les aplicacions desenvolupades hauran d'integrar-se completament amb el MiB, de manera que s'hauran de crear les interfícies necessàries amb el mateix. Tanmateix, el Pla de Proves del projecte haurà de definir un conjunt de proves específiques que permetin comprovar la correcta connectivitat entre l'aplicació desenvolupada i el MiB.

BIT posa a disposició de l'empresa proveïdora el catàleg des serveis actualment disponibles a través del MiB.

4.3.1. Sistema de Coordenades de Referència

Les coordenades que s'enregistrin al Sistema d'Informació han de ser acords al sistema geodèsic de referència anomenat ETRS89 (European Terrestrial Reference System 1989), establert com a oficial pel Decret 1071/2007 i basat en l'el·lipsoide GRS80 (Geodetic Reference System 1980), consistent amb els actuals sistemes de posicionament per satèl·lit.

La representació planimètrica serà l'establerta com a reglamentària pel Decret 1071/2007, a Catalunya serà la projecció UTM31N (coordenades x,y).

El codi EPSG (European Petroleum Source Group) s'utilitza per a identificar el Sistema de Coordenades de Referència (CRS) de les coordenades emprades en un conjunt de dades, en aquest cas, el codi que aplica és el EPSG:25831 (projecció UTM ETRS89, fus 31 Nord).

Quant s'hagin de mostrar coordenades a la persona usuària, s'haurà de fer en aquest format (exemple):

Coordenades UTM - ETRS89 (m) : 432.417,598; 4.583.997,889

Les coordenades d'objectes geomètrics (punts, línies, polígons) emmagatzemades en bases de dades Oracle hauran de seguir el format *Oracle Spatial* i estar en un camp de tipus SDO_GEOMETRY que s'anomenarà, preferentment, GEOMETRIA, i amb el SRID informat. D'acord amb les especificacions, també caldrà definir les metadades *Spatial* i que al camp GEOMETRIA hi hagi un índex espacial.

4.3.2. Geocodificació d'adreces

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

La Geocodificació fa referència a:

- Validació, normalització i obtenció d'adreces postals
- Obtenció de carrer-numero, escala-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.

La validació d'adreces i consulta de dades relacionades amb la geocodificació es realitzarà en els aplicatius a partir dels serveis transversals o mòduls comuns que disposa BIT i que recobreixen l'accés a la base de dades GEOCOD (en referència a l'esquema SDR_GEOCOD, en ETRS89). Depenent de l'entorn de desenvolupament i el tipus d'integració que es requereixi, es farà a partir d'algun d'aquests sistemes:

- Accés directe al Package PL/SQL de la GEOCOD (opció menys recoberta)
- Serveis web GeoREST
- API Geocomponents (GeoBCN) (opció més recoberta i recomanada quan es necessita visualitzar cartografia)

En tots els aplicatius nous, es treballarà amb el Sistema de Coordenades de Referència ETRS89. D'altra banda, cal esmentar que sempre s'evitarà el duplicar dades i nomes s'emmagatzemaran codis, mai descripcions (Ex. S'ha d'emmagatzemar el codi de carrer en comptes del nom de carrer, que és una descripció).

Els processos de geocodificació dels serveis en 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 polígons de vialitat.

BIT proporcionarà la documentació tècnica i una guia d'ús i bones pràctiques relacionades amb la geocodificació que s'hauran d'acomplir.

4.3.3. Bases cartogràfiques i geo-serveis

Els aplicatius en els que s'hagi de mostrar cartografia, hauran de fer servir les bases oficials de l'Ajuntament de Barcelona, i només en aquells casos que estigui suficientment justificat, excepcionalment es faran servir altres bases, com ara la d'Open Street Maps, o la cartografia de Google.

A tal efecte, BIT disposa de la infraestructura pròpia de publicació de mapes per tal d'exposar les capes d'informació geoespacial al visors cartogràfics de les aplicacions que es desenvolupin.

D'una banda es proporcionen diferents Web Services per servir mapes d'acord al protocol estàndard WMS (Web Map Service) de l'OGC (Open Geospatial Consortium, www.opengeospatial.org). La relació actual de serveis disponibles es pot consultar en http://www.bcn.cat/geoportal/ca/geoserveis.html, i es podrà ampliar en aquells serveis necessaris si es que els requereix el projecte. Dins d'aquesta llista de geo-serveis, també s'ofereixen serveis de mapes pre-cachejats, o el que es coneix com a serveis tessel·lats, en aquest cas acords al protocol estàndard WMTS (Web Map Tile Service).

Mentre que els serveis WMS ofereixen la cartografia en "temps real", és a dir, representen allò que hi ha emmagatzemat a les bases de dades just en el moment de la consulta, els serveis WMTS, i tessel·lats en general, ofereixen el contingut d'una caché pre-generada. La freqüència d'actualització d'aquests continguts és diferent segons el servei en concret. La pre-generació obeeix a requeriments d'aplicatiu quant a temps de resposta i rapidesa en la navegació pel mapa.

BIT també publica de manera directa diferents col·leccions de cartografia tessel·lada, a diferència dels serveis WMTS, sense que intervingui cap servei, atès que el contingut i la localització de les tessel·les estan configurades prèviament. Aquest mètode de localització de tessel·les es coneix com a direccionalment XYZ. Hi han diferents esquemes per a identificar aquest direccionalment, dels quals BIT ofereix mapes amb l'especificació TMS (Tile Map Service Specification) i amb l'especificació Google XYZ en projecció pseudomercator codificada com a EPSG:3857, que serà la que prevaldrà pel seu ús més generalitzat. Dins d'aquestes col·leccions es disposa del mapa del Plànol de Barcelona, Topogràfic i mapes urbanístics.

Al igual que amb la resta de serveis de mapes, les col·leccions tessel·lades es podran ampliar amb nous mapes amb els continguts necessaris si es que els requereix el projecte.

4.3.4. Mòduls comuns de visualització cartogràfica (entorn web)

BIT proporciona dos marcs o mòduls comuns de desenvolupament per aplicacions amb visor cartogràfic en web, en entorns navegador Desktop i Mobile (responsive):

API Geocomponents (GeoBCN):

El primer, i com a opció de preferència, és un API JavaScript sobre base de codi obert que proporciona un conjunt de components i serveis RESTful que permeten visualitzar elements cartogràfics sobre diferents fons de base (capes vectorials, tessel·lades i serveis WMS interns/externs), cercar elements i obtenir informació alfanumèrica d'aquests. Es tracta dels GeoComponents: solució API que recobreix el codi obert OpenLayers 5 i que aporta, a més de la visualització, un seguit de serveis RESTful de consulta de dades referents a posicionament i geocodificació. Es pot accedir a l'API, la seva documentació i els seus exemples a https://w33.bcn.cat/GeoBcn

Aquelles funcionalitats addicionals que requereixi el projecte i que no estiguin contemplades en GeoBCN, s'implementaran de manera genèrica com a part integrant d'aquest mòdul comú. BIT facilitarà les pautes tècniques i organitzatives per poder fer aquesta integració.

Existeix un segon nivell de recobriment d'aquest mòdul, que s'utilitza per integrar directament en una aplicació web un frame amb la cartografia del Plànol de Barcelona i la imatge aèria, proporcionant les eines bàsiques de navegació i la possibilitat de dibuixar marques de posicionament o "xinxetes". Aquest mòdul és el Widget del Plànol. De la mateixa manera, es pot accedir a l'API, la seva documentació i els seus exemples a https://w33.bcn.cat/planolBCN/widget_i/index.html

Components de la Infraestructura de Dades Espacials:

El segon marc comú són els components del Geoportal i de la Infraestructura de Dades Espacials (Web Map Publisher Services), basada en tecnologia propietària i que permeten incloure un visor capaç de mostrar sobre fons de base de diferent origen múltiples fonts de dades interoperables acords als estàndards, com Open Street Maps, Google Maps, GeoRSS, Open Location Services, WMS, WFS, WFS-G, serveis tessel·lats WMTS o XYZ, etc.

4.4. 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 BIT (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 BIT.
- Aquells establerts o definits en la fase de presa de requeriments del contracte.

4.4.1. Seguretat de l'aplicació

RS2. [Obligatori] Autenticació: El sistema ha de comprovar que la persona usuària que tracta d'accedir al sistema és qui diu ser. De forma general, l'autenticació de les persones usuàries es pot fer mitjançant els següents mecanismes:

- Codi 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 persones usuàries 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 les persones usuàries d'aquest sistema amb les persones usuàries 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 la persona usuària amb el sistema es realitzarà únicament mitjançant canals segurs (https). Els algoritmes criptogràfics emprats seran els acreditats pel Centre Criptològic Nacional per al seu ús en l'Esquema Nacional de Seguretat.

RS6. [Obligatori] Gestió de persones usuàries i sessions: Els mecanismes de control de sessions de persones usuàries autenticats contemplaran:

a. Tancament de sessió per part de la persona usuària.

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 la persona usuària.

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 desencriptaran

per ser llegides un cop comprovat que la persona usuària té el perfil necessari per veure-les.

- BIT indicarà quin algoritme s'ha de fer servir en cada cas.

4.4.2. Control d'accés

El model de control d'accés haurà de complir amb els requeriments establerts per l'Oficina de Govern de Seguretat (OGS) de BIT que és qui té la competència en matèria de Gestió d'Identitats Digitals i Control d'Accés dins l'Administració Municipal.

Aquests processos han de ser compatibles amb la Gestió d'identitats (GID).

La solució de Gestió d'Identitats de l'Ajuntament de Barcelona (GID) es basa actualment en Oracle identity manager 11 i Oracle Access Manager. En el moment de confecció d'aquesta versió del document, a BIT s'està en procés de decomisió d'aquesta solució i en procés d'implantació amb l'IdP (Identity provider) de l'Ajuntament de Barcelona. En concret, actualment aquest està basat en el producte RedHat Single Sign ON (Keycloak). En subapartat existeix detall concret.

El Control d'Accés a les aplicacions dins de la Xarxa Municipal es basa en codi de persona usuària i contrasenya.

El Control d'Accés des d'internet es basa en l'ús de Certificats Digitals.

La codificació dels identificadors de persona usuària ha de seguir els estàndards d'identitat corporativa establerts per l'Oficina de Govern de Seguretat (OGS).

La política de caducitat de contrasenya i fortalesa de les mateixes serà l'establerta de forma corporativa per l'Oficina de Govern de Seguretat (OGS).

Donat que el nivell de seguretat d'alguns mòduls respecte a la LOPDGDD han estat considerats de nivell alt. D'acord amb el RLOPD 1720/2007 art. 103 s'hauran de registrar els intents d'accés infructuós.

4.4.2.1. IDP

El projecte podrà fer servir un dels següents protocols d'autenticació/autorització permesos:

- OpenID Connect (Oauth2) per aplicacions desenvolupades a mida i productes
  - Aplicacions Client: Code Flow amb PKCE (amb Intercanvi d'una clau codificada)
  - Aplicacions de backend (per consumir altres backends): Client Credentials Flow
- SAML per a productes sempre que no suportin OpenID Connect

El token rebut per les aplicacions tindrà aquest format:

ACCESS_TOKEN de resposta

{
"alg": "RS256",
"typ": "JWT",
"kid": "ZLtfmyx_ZYZKLcn0olLU_VtWCLjSC9R-vG91CXEBQi0"
}
{
"exp": 1690526988,
"iat": 1690526688,
"jti": "db4bcc38-b5cf-4e03-9b8a-7676d08a9799",
"iss": "https://idp-int.ajuntament.bcn/auth/realms/corp",
"sub": "5fea02ff-5ce4-408b-9c1a-b180fa9c9bc4",
"typ": "Bearer",
"azp": "testapp",
"session_state": "74c29232-cf16-4faf-a997-9a17faa45eef",
"**resource_access**": {
"testapi": {
"roles": [
"READ"
]
}
},
"scope": "openid testapi",
"sid": "74c29232-cf16-4faf-a997-9a17faa45eef",
"givenName": "Roberto",
"sn": "Test",
"user": "testtest",
"version": "1",
"email": "testtest@test.es"
}

Els roles vindran en el claim "**resource_access**" que serà un array d'arrais amb tots els roles dels clients demanats la petició. La forma de demanar-ho és a través dels scopes. Cada api tindrà un scope propi per demanar els seus roles al token.

4.4.3. Gestió de les Autoritzacions

Les autoritzacions han de seguir un model RBAC (Role Based Access Control) que haurà de ser validat pels/per les responsables tecnològics dels serveis i per l'Oficina de Seguretat TIC.

El model proposat haurà de complir amb els següents principis:

- Segregació de funcions
- Mínim privilegi
- Necessitat de Conèixer

- Economia d'Administració
- Usabilitat

La gestió de permisos haurà de ser en base a perfils i rols, podent una persona usuària tenir múltiples perfils. Les persones usuàries 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.

S'hauran de poder gestionar permisos per criteris organitzatius i de negoci (per exemple, execució de treballs i certificació de treballs).

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.

Per facilitar l'administració s'hauran de poder gestionar els permisos mitjançant plantilles de seguretat, entenent com a plantilla una agrupació de perfils.

El model ha de contemplar un perfil per persona usuària final que permeti la gestió dels permisos per aquelles persones que des de negoci tinguin el rol de "Responsable de Control d'Accessos" d'acord amb la definició que ha fet la Comissió Tècnica de Seguretat i Protecció de Dades de l'Ajuntament de Barcelona.

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

4.4.4. 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 de persona usuària, 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 ples persones usuàries que puguin afectar a informació sensible, i permeti a una persona amb l'autorització adequada accedir fàcilment a l'historial d'operacions realitzades per una persona usuària, així com a l'historial d'operacions realitza sobre un objecte.

4.4.5. 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'empresa adjudicatària s'ha de comprometre també a adaptar el Manual d'Explotació d'aquestes traces.

Amb tal propòsit, l'empresa adjudicatària haurà de dissenyar les traces necessàries en base al Document del 'Pla de Seguretat i Traces' que posarà a disposició BIT 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.

4.4.6. 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'empresa adjudicatària s'abstindrà d'utilitzar dades reals per fer proves.

Per tant, l'empresa adjudicatària 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/de la 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'empresa adjudicatària i s'incorporaran al contracte com una funcionalitat més que a la finalització del mateix quedarà a disposició de l'equip tècnic de BIT.

4.4.7. 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 BIT d'acord amb la seva potestat d'autoorganització.

4.5. Estàndards de desenvolupament

4.5.1. Per a tecnologia J2EE

4.5.1.1. Aplicacions Arquitectura 2020 (OpenFrame4)

Es farà servir aquesta arquitectura per noves aplicacions.

Per implementar aquesta arquitectura BIT utilitza:

- El Framework openFrameBIT o altres tecnologies com per exemple Quarkus o prescindir de l'ús d'openFrameBIT i usar Springboot natiu.
- Els components d'ús general de BIT.
- Els elements de programació de l'especificació J2SE 1.7 i Spring Framework 4.0

L'empresa adjudicatària pot utilitzar OpenFrameBIT a la seva darrera versió pel desenvolupament dels productes del contracte desenvolupats en tecnologia J2EE/J2SE de manera opcional.

A més de l'estructura lògica dels components segons el patró MVC, OpenFrameBIT divideix els seus components en una arquitectura de 3 capes:

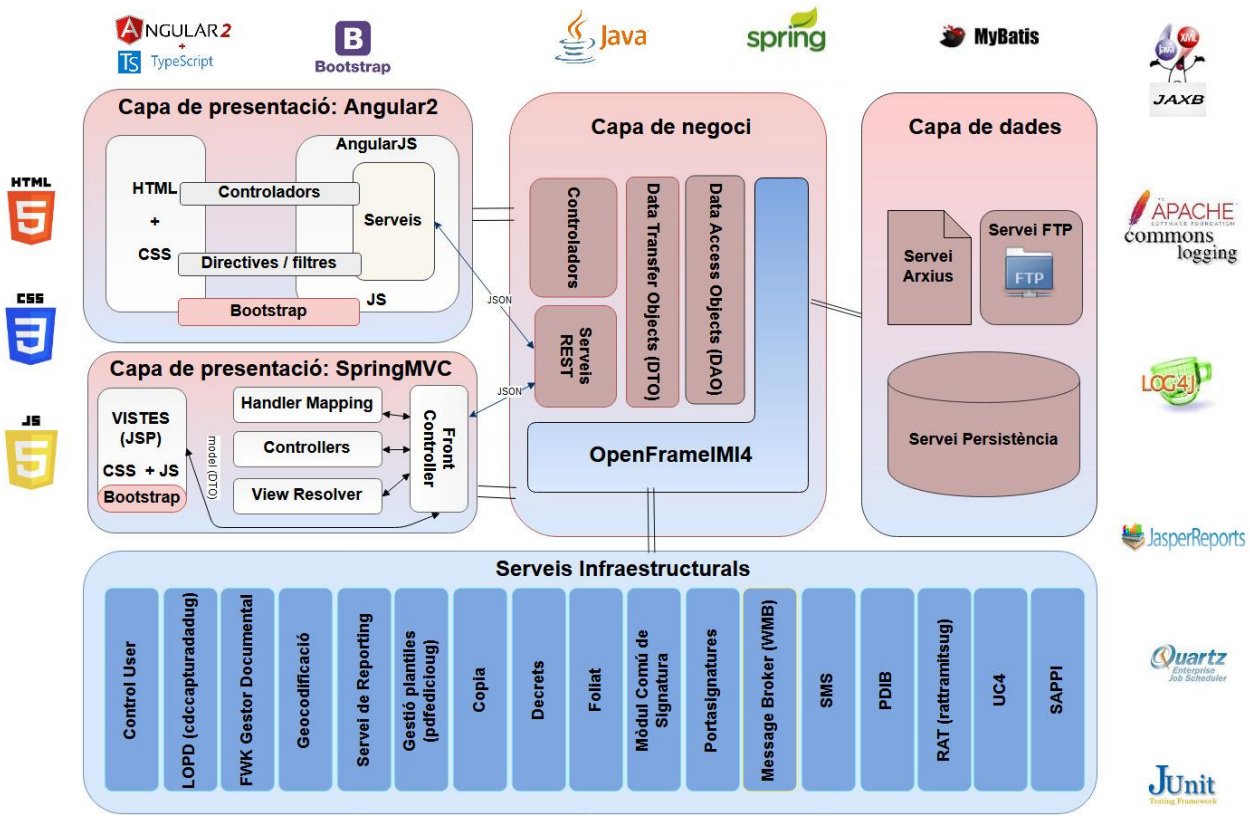
- Capa de Presentació. La implementació concreta d'aquesta capa **no ve fixada pel framework.**

- Capa de Lògica de Negoci.
- Capa d'Integració i Accés a Dades.

En cadascuna d'aquestes capes s'han definit diferents serveis que es mostren en el gràfic de la pàgina següent. A més dels serveis propis de cadascuna de les capes s'ofereixen Serveis de Propòsit General, adequats per a qualsevol de les capes. Tots els serveis es troben definits mitjançant interfícies, quedant així aïllats dels desenvolupaments concrets.

Els diferents serveis es troben empaquetats en llibreries jars diferents. Això ofereix l'avantatge que cada aplicació únicament cal que disposi de les llibreries que necessita. Per tant quan es desenvolupen noves aplicacions únicament cal centrar els esforços en el desenvolupament de les accions i les funcionalitats de Negoci.

Els serveis i la base tecnològica utilitzats per OpenFrame4 es poden representar de la següent manera:



Aquest gràfic recull la major part dels serveis disponibles a BIT, però no necessàriament tots ells. Les empreses licitadores que ho creguin necessari, poden demanar a BIT la informació detallada dels mateixos.

OpenFrame4 **no és el/la responsable** dels estils de presentació, aquests depenen del que determini la Direcció Técnica d'Internet i la persona usuària final.

OpenFrame4 **no ofereix** serveis de presentació que agilitzen la construcció d'aplicacions, sinó que dona les pautes per la seva utilització. Es donen diferents opcions pel que fa a la implementació de la capa client:

- **AngularJ2 :** Es farà servir per desenvolupar les aplicacions Single Page Application (SPA) de l'Ajuntament.

  Angular implementa un patró derivat del MVC, el patró MVVM (model-view-viewmodel). En aquest patró el controlador és substituït per l'anomenat "viewmodel", que té les mateixes responsabilitats però que inclou un "binder", que s'encarrega de manera automàtica de sincronitzar les dades del model i de la vista, alliberant al desenvolupador de fer-ho mitjançant programació imperativa. Disposa d'un mòdul que permet fàcilment consumir les APIs REST dels back-ends des dels serveis.

  Tot i que Angular ens dona els mecanismes per definir components, en principi cal començar de zero, definint els seus templates HTML i estils CSS. Per evitar-ho, farem servir Bootstrap ja que és un framework per al disseny de pàgines i aplicacions web que proporciona controls visuals amb els seus estils, comportaments i animacions.

  A més BIT proporcionarà una sèrie de components "typescript" amb la seva documentació i estils propis acordats amb la Direcció Tècnica d'Internet (DTI), la documentació d'aquests components, com tota la resta de documentació, estarà actualitzada a la wiki del departament d'arquitectura.

- **SpringMVC**: Mòdul de Spring que facilita el desenvolupament d'aplicacions web basant-se en els patrons de disseny: MVC i Front Controller.

  Caldrà tenir present com amb la opció anterior la utilització dels estils de presentació acordats amb la DTI (Direcció Tècnica d'Internet).

- **Altres (JSF, etc.)**

Pel que fa a la capa de negoci, en cas de ser necessaris sí s'hauran d'utilitzar els serveis comuns comentats anteriorment.

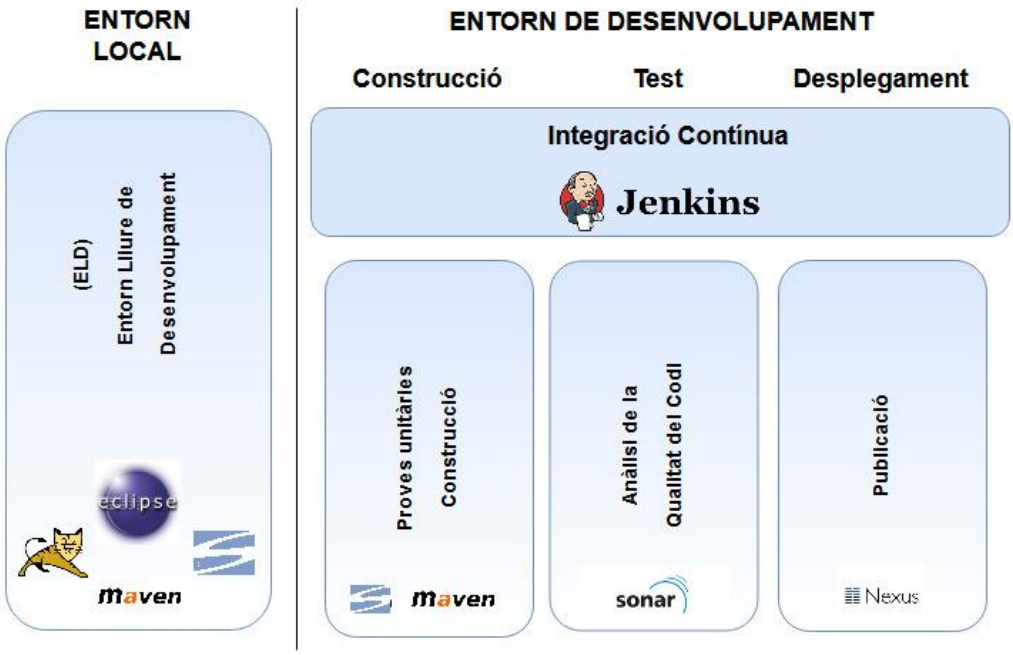
Els estàndards i guies J2EE existents a BIT determinen diferents aspectes com:

- Els entorns de desenvolupament on s'han de provar i posar en funcionament les aplicacions J2EE.
- Les eines de desenvolupament que es disposen.
- La tipologia dels fitxers que composen les aplicacions, la seva nomenclatura i els directoris on s'han de col·locar segons els tipus.
- Els passos a seguir durant el desenvolupament, tenint en compte tant la creació de noves aplicacions com la modificació de versions existents.

- El manual d'ús d'OpenFrameBIT, que inclou l'explicació del detall de l'arquitectura base i la guia d'us per a cada servei.

Pel que fa a les eines de desenvolupament cal destacar la utilització a BIT de les següents eines de treball:

- Per l'entorn de desenvolupament LOCAL es proporciona un **ELD** (Entorn Lliure de Desenvolupament).
  Aquest Entorn de Desenvolupament Integrat és realment un **Eclipse** integrat amb l'eina de gestió de codi font (**GIT**).
  S'integra també amb **Maven** i utilitza el servidor **Tomcat** per poder desplegar i provar les aplicacions que es realitzin.



- Pel desplegament i construcció es fa servir una eina pròpia, l' "**Orquestrador**" de AjBcn, que internament s'integra amb:
  - Eina de gestió de codi (actualment **GIT**). Fent servir jobs de **jenkins** s'utilitza **maven** per poder construir els artefactes necessaris pel desplegament arrel de qualsevol número de revisió de **GIT**.
  - Eina per garantir el manteniment continu de la qualitat del codi (**Sonar**). Executa una sèrie de regles definides per BIT per tal d'assegurar una qualitat contínua del codi entregat.
  - Repositori d'artefactes (**Nexus**). Eina que es fa servir per publicar i mantenir les diferents versions dels artefactes generats.
  - Eina d'integració contínua (**Jenkins**). Permet realitzar la integració del DPL amb la resta d'eines de gestió contínua mencionades anteriorment.

Pel desplegament als entorns de desenvolupament i pre-producció els AM son autònoms per les execucions. Per el desplegament a entorn productiu s'ha de tramitar mitjançant petició EasyVista per seguiment i participació dels equips Gestió del Canvi i Gestió de Versions.

4.5.1. Per a tecnologia Python

4.5.1.1. Introducció

Aquest document pretén ser una guia de referència per al desenvolupament d'aplicacions Python a BIT.

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.

4.5.1.2. 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.

4.5.1.2.1. 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.

4.5.1.2.2. 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.

4.5.1.2.3. 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.

4.5.1.3. 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.

4.5.1.4. 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 prevists 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.

4.5.1.4.1. 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	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.

	DP11	
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 *backends* d'emmagatzemament de medies en diferents entorns (AWS S3, Google Cloud...)

4.5.1.5. 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 medies privats

4.5.1.5.1. 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

4.5.1.6. 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 prevists 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.

4.5.1.6.1. 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

4.5.1.7. 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.

4.5.1.7.1. 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

4.5.1.8. 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.

4.5.1.8.1. 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 *Built-in* (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 *Virtualenv*, permet validar de manera automàtica les llicències dels paquets i aplicacions emprats per un projecte.

4.6. Metodologia de desenvolupament

4.6.1. Qualitat de codi

RQ1. Tot codi font que es vulgui desplegar als servidors de BIT requerirà el compliment dels estàndards de qualitat indicats pel mateix BIT. Aquests estàndards es concreten en l'aplicació de diferentes Quality Gates.

Quality Gates actuals per Java:

- Conditions on New Code
  - **Coverage**, ha de ser superiror 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'empresa adjudicatària del servei.

RQ3. En cas d'aplicacions antigues, no desenvolupades des del seu inici amb els actuals llindars de qualitat, es marquen els mateixos llindars, però donada la complexitat d'adaptació que pot suposar s'estableix flexibilitat al respecte.

En el moment de confecció actual d'aquest document no s'aplica el control de qualitat de codi a les aplicacions "antigues" y es preveu que en breu temps es comencin a aplicar les mateixes regles però **només per al codi nou.**

RQ4. En qualsevol cas l'empresa proveïdora 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. BIT podrà exigir que el **nou codi** compleixi amb la regla del 60% de Cobertura. No obstant això, l'empresa proveïdora podrà demanar la relaxació d'aquest llindar 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 llindar serà inferior al 30% de Cobertura de codi.

4.6.2. 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 BIT.

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 BIT.

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:

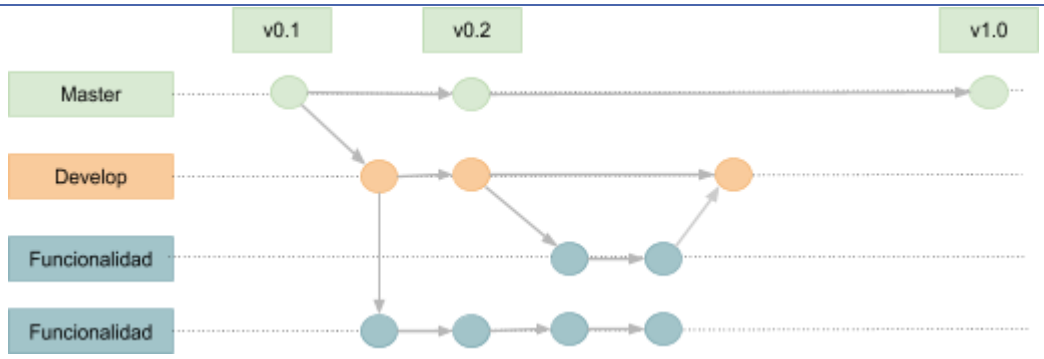


FIG. 2 – FLUX GENERAL DE DESENVOLUPAMENT

4.6.3. 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 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 de persona usuària: aquests ens serviran per garantir que la interfície de persona usuària 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.

5. CLÀUSULES GENERALS DE SEGURETAT

BIT 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 de les empreses licitadores sota demanda. L'empresa proveïdora 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.

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

Les empreses licitadores s'obliguen a vetllar pel compliment de la legislació vigent aplicable a l'objecte del contracte i especialment pel 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 BIT indistintament. De conformitat als seus estatuts s'ha d'entendre que BIT 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.

5.1. Responsable de seguretat

L'empresa adjudicatària 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 per l'empresa proveïdora a l'Ajuntament es realitzen d'acord al model i requeriments de seguretat establerts per BIT 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 BIT.

- Assegurar que tot el personal de l'empresa adjudicatària que prestarà serveis a l'Ajuntament, passi per un pla de conscienciació i formació en matèria de seguretat.

- Assegurar que tot el personal de l'empresa proveïdora que hagi de tractar dades o sistemes de tractament de dades de nivell sensible o superior signin un Acord de Confidencialitat Individual. BIT 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.

5.2. 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.

5.3. Auditoria

BIT auditarà que l'empresa adjudicatària vetlli per la qualitat del seu servei. Es contemplen dos tipus d'auditories:

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

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

L'empresa adjudicatària proporcionarà l'assistència i la informació que requereixin les auditories, sense càrrec addicional per a BIT.

La realització de l'auditoria en cap moment eximirà l'empresa adjudicatària 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'empresa adjudicatària, d'acord amb el calendari establert al pla d'acció, es compromet a portar a terme les activitats establertes en el pla d'acció. BIT podrà verificar que el pla d'acció s'ha implementat correctament.

5.4. Gestió d'Incidents de Seguretat

L'empresa adjudicatària informarà a BIT-Seguretat de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert per BIT.

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

5.5. Confidencialitat

L'empresa adjudicatària 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'empresa adjudicatària 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'empresa adjudicatària 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'empresa adjudicatària 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.

5.6. Dimensionament/gestió de capacitats

L'empresa proveïdora disposarà del personal necessari amb les qualificacions professionals adients, per a la prestació del servei de forma adequada.

5.7. 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'empresa adjudicatària té prohibit incorporar les dades a altres sistemes o suports sense autorització expressa i haurà de complir amb les mesures de seguretat establertes per BIT.

5.8. Anàlisis forenses

L'execució d'anàlisis forenses és responsabilitat exclusiva de BIT-Seguretat. L'empresa adjudicatària 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 BIT-Seguretat i l'empresa proveïdora.

5.9. Control d'accés

5.9.1. Accés local

L'empresa adjudicatària 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 la persona usuària de les seves obligacions immediatament després d'obtenir l'accés.
- S'informarà a la persona usuària de l'últim accés efectuat amb la seva identitat.

5.9.2. Accés remot

L'empresa adjudicatària 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 BIT per als sistemes de l'Ajuntament.

5.10. Gestió del Personal

5.10.1. 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 pertoqui i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Ajuntament.

El/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'acceptació de les obligacions signat per les persones adscrites a l'execució d'aquest contracte serà entregat al Cap de Projecte de l'Ajuntament, abans de ser donats els permisos per accedir als Sistemes d'Informació de l'Ajuntament o bé abans de ser facilitada la informació per al correcte compliment del servei contractat, i restarà en poder de l'empresa adjudicatària que haurà de presentar-los quan siguin requerits per l'Ajuntament.

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

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

5.10.2. Formació i conscienciació

L'empresa adjudicatària 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'empresa adjudicatària 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'empresa adjudicatària ha realitzat sobre el personal assignat a l'execució del contracte.

5.11. Protecció del lloc de treball

5.11.1. Lloc de treball buit

L'empresa adjudicatària 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.

5.11.2. Bloqueig del lloc de treball

L'empresa adjudicatària garantirà que els seus equips es bloquejaran al cap d'un temps prudencial d'inactivitat, requerint una nova autenticació de la persona usuària per reprendre l'activitat.

5.11.3. Protecció d'equips

L'empresa adjudicatària 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'empresa adjudicatària 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. Les persones usuàries hauran de disposar d'un canal de de comunicació per informar al servei de gestió d'incidents de pèrdues o robatoris, que hauran de ser comunicades a BIT.

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

Addicionalment, els equips hauran de disposar:

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

5.11.4. Medis alternatius

L'empresa adjudicatària 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.

5.12. Clàusula de comunicacions externes

L'empresa adjudicatària 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'empresa adjudicatària serà el/la 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.

5.13. Protecció dels Suports Informàtics

L'empresa adjudicatària haurà de gestionar els suports informàtics amb informació de l'Ajuntament de Barcelona seguint les següents pautes.

5.13.1. Etiquetat

L'empresa adjudicatària 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. Les persones usuàries 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.

5.13.2. 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 BIT-Seguretat.

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents amb la informació municipal o corporativa, l'empresa adjudicatària haurà de presentar-les per ser validades per BIT-Seguretat i/o seguir els estàndards i normes de BIT.

5.13.3. Transport

L'empresa adjudicatària 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'empresa adjudicatària 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.

5.13.4. Esborrat i destrucció

L'empresa adjudicatària haurà de seguir els estàndards i normes de BIT 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 de 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 BIT.

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.

5.14. Protecció de la Informació

5.14.1. Neteja de documents

L'empresa adjudicatària 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.

5.14.2. Protecció del correu electrònic

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

- La informació distribuïda per mitjà de correu electrònic, es protegirà, tant en el cos dels missatges, com en els annexos.
- Es protegirà la informació d'encaminament de missatges i establiment de connexions.

- No es permetrà la redirecció a dominis de correus públics fora del correu corporatiu de l'empresa adjudicatària.
- 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'empresa adjudicatària establirà polítiques d'ús del correu electrònic que inclourà com a mínim:

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

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

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

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

5.15. Protecció de les instal·lacions

Les instal·lacions de l'empresa adjudicatària 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.

5.16. 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 BIT-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.

5.17. Protecció de dades de caràcter personal

L'empresa adjudicatària, 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/de la responsable.
- Portar, per escrit, un registre de totes les categories d'activitats de tractament efectuades per compte del/de la 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/de la 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/de la 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/la 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/per la 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/de la 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/la responsable, com a mínim:

      1. La naturalesa de la violació de les dades.

      2. Dades del punt de contacte del/de la 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/per la 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/de la 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/la responsable o un altre auditor autoritzat per ell.
- Permetre i contribuir a la realització d'auditories, incloses inspeccions, per part del/de la 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 rebi 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/de la 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'autoritzés 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/la 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.

5.18. Clàusules d'administració de producte

5.18.1. Gestió d'identitats, autenticació de persones usuàries

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

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

Autenticació interna

Les persones usuàries interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per BIT basats en protocols estàndards de seguretat. L'empresa proveïdora haurà d'assegurar que s'utilitzi el repositori central per a l'autenticació de les persones usuàries. La solució d'autenticació corporativa utilitzada per BIT és l'Oracle Access Manager (OAM) que proveeix el Single Sign On corporatiu.

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

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

Autenticació externa

Les persones usuàries 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, requerint així una verificació de la identitat de l'usuari que sol·licita accés. Actualment, la solució implantada al BIT fa ús de Google Authenticator.

5.18.2. Autorització de les persones usuàries als sistemes

BIT disposa d'un mecanisme d'autorització de persones usuàries corporatiu basat en el producte Oracle Unified Directory (OUD). L'empresa adjudicatària haurà d'assegurar que les autoritzacions es troben delegades en el repositori central d'autorització (OUD).

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

La integració d'aquest connector anirà a càrrec de l'empresa adjudicatària i comptarà amb el suport i la supervisió de l'equip de gestió d'identitats. El temps dedicat normalment a integrar un connector estàndard amb una BBDD Oracle és aproximadament 80 hores d'un tècnic.

Perfilat de persones usuàries

Les autoritzacions han de seguir un model RBAC (Role Based Access Control) que haurà de ser validat pels/per les responsables tecnològics de la plataforma i per BIT-Seguretat.

El model proposat haurà de complir amb els següents principis:

- Segregació de funcions, de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.
- Mínim privilegi, els privilegis de cada persona usuària es reduiran al mínim estrictament necessari per complir les seves obligacions.
- Necessitat de Conèixer, els privilegis es limitaran de manera que les persones usuàries 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 una persona usuària tenir múltiples perfils. Les persones usuàries 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'empresa adjudicatària 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'empresa adjudicatària per incloure nous punts a tractar o adaptacions dels punts existents.

5.18.3. Inventari d'actius

L'empresa adjudicatària 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.

5.18.4. Configuració de seguretat

L'empresa adjudicatària 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 la persona usuària i protegiran a aquest, tret que s'exposi conscientment a un risc.
    - Per reduir la seguretat, la persona usuària ha de realitzar accions conscients.
    - L'ús natural, en els casos que la persona usuària no ha consultat el manual, serà un ús segur.

5.18.5. Manteniment

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

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

L'empresa proveïdora 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.

5.18.6. 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 BIT-Seguretat. BIT-Seguretat ha d'assegurar la disponibilitat de la informació als propietaris d'aquesta dins de l'Ajuntament. BIT-Seguretat custodiarà les claus de xifratge.

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents amb la informació municipal o corporativa, l'empresa proveïdora haurà de presentar-les per ser validades per BIT-Seguretat i/o seguir els estàndards i normes de BIT.

5.18.7. Certificats

BIT-Seguretat serà el/la responsable de la custòdia i protecció dels certificats digitals emesos en nom de l'Ajuntament de Barcelona a través de BIT-Seguretat. 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 BIT-Seguretat per al seu control i gestió.

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

5.18.8. Antimalware

L'empresa adjudicatària serà responsable de la instal·lació i actualització de programes de protecció antimalware de les màquines que suporten serveis de BIT segons es recull al marc normatiu de BIT.

BIT 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.

BIT seguretat tindrà accés en consulta a la consola de gestió d'aquests programaris de l'empresa proveïdora.

5.18.9. Còpies de seguretat

L'empresa adjudicatària 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 BIT.

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, BIT es reserva el dret de demanar el xifrat de les dades. L'abast de les còpies inclou:

- Informació de treball de BIT.
- 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'empresa adjudicatària 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.

5.18.10. Segregació de funcions i tasques

L'empresa adjudicatària 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.

5.18.11. Explotació

5.18.11.1. Gestió de la configuració

L'empresa adjudicatària 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.

5.18.11.2. Gestió de canvis

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

- Tots els canvis anunciats per l'empresa fabricant o empresa proveïdora 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.

5.18.11.3. Protecció de claus criptogràfiques

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

5.18.12. Protecció dels serveis

5.18.12.1. Protecció enfront de la denegació de servei

L'empresa adjudicatària 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.

5.18.12.2. Protecció de les aplicacions i serveis web

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

- Quan la informació tingui algun tipus de control d'accés, es garantirà la impossibilitat d'accedir a la informació obviant l'autenticació, en concret prenent mesures en els següents aspectes:
    - S'evitarà que el servidor ofereixi accés a documents per vies alternatives al protocol determinat.
    - Es previndran atacs de manipulació 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'autentificació de llocs web d'acord amb les polítiques establertes per BIT-Seguretat.

5.19. Clàusules de desenvolupament de producte

5.19.1. Clàusula de propietat intel·lectual

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

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

L'empresa contractada accepta expressament que els drets d'explotació dels productes derivats d'aquest plec corresponen única i exclusivament a l'Ajuntament de Barcelona. Així doncs, el contractat cedeix, amb caràcter d'exclusivitat, la totalitat dels drets d'explotació dels treballs objecte d'aquest plec, inclosos els drets de comunicació pública, reproducció, transformació o modificació i qualsevol d'altre dret susceptible de cessió en exclusiva, d'acord amb la legislació sobre drets de propietat intel·lectual.

5.19.2. Clàusula programari i metodologia de desenvolupament

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

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

L'Administració Municipal continuarà essent la propietària o, en el seu cas, titular dels drets de propietat intel·lectual que el corresponen sobre el programari i bases de dades instal·lat en les màquines de l'empresa contractada, sense que la corresponent llicència d'ús suposi transferència o cessió, total o parcial de la titularitat, ni autorització per la seva utilització amb una finalitat diferent a la definida en el contracte de prestació de serveis.

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

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

5.19.3. Desenvolupament segur

L'empresa adjudicatària 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.

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

Per a millorar el procés de desenvolupament segur d'aplicacions, l'empresa adjudicatària 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/la responsable del contracte. El software emprat a BIT correspon a l'eina SonarQube amb la modalitat OWASP, sent aquesta la tecnologia desitjable a emprar per l'empresa adjudicatària.
- Per al cas particular d'aplicacions conteneritzades, l'empresa adjudicatària haurà de fer ús d'un software d'anàlisi d'imatges Docker. La tecnologia emprada a BIT i la preferent d'ús per part de l'empresa adjudicatària és Coreos Clair.

En cas d'emprar softwares diferents als plantejats anteriorment, hauran de ser comunicats i justificats degudament al responsable del contracte.

5.19.4. Acceptació i posta en servei

Abans de passar a producció l'empresa adjudicatària 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.

Addicionalment, l'empresa adjudicatària realitzarà les següents inspeccions prèvies a l'entrada en servei:

- Anàlisi de vulnerabilitats.
- Test de penetració.

5.19.5. Protecció de les aplicacions i serveis web

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

- Quan la informació tingui algun tipus de control d'accés, es garantirà la impossibilitat d'accedir a la informació obviant l'autenticació, en concret prenent mesures en els següents aspectes:
    - S'evitarà que el servidor ofereixi accés a documents per vies alternatives al protocol determinat.
    - Es previndran atacs de manipulació de URL.
    - Es previndran atacs de manipulació de fragments de la informació que s'emmagatzemin en el disc dur del visitant d'una pagina web a traves del

seu navegador, a petició del servidor de la pagina, conegut en la terminologia anglesa com a “cookies”.

- Es previndran atacs d’injecció de codi.

- Es previndran intents d’escalat de privilegis.
- Es previndran atacs de “cross site scripting”.
- Es faran servir certificats d’autentificació de llocs web d’acord amb les polítiques establertes per BIT-Seguretat.

5.19.6. Dades de proves

L’empresa adjudicatària 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’empresa adjudicatària 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’empresa adjudicatària 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.

5.19.7. Signatura electrònica

Qualsevol requeriment de signatures digitals que s’hagin de produir referents amb la informació municipal o corporativa, l’empresa proveïdora haurà de presentar-les per ser valides per BIT-Seguretat i/o seguir els estàndards i normes de BIT.

Per la signatura electrònica s’empraran els mecanismes aprovats per BIT, en cas que hagin de ser uns altres, s’haurà de justificar, documentar tècnicament i haurà d’estar validat per BIT-Seguretat. En tot cas s’ha de complir la política de signatura electrònica de l’Ajuntament de Barcelona.

5.19.8. 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'empresa adjudicatària haurà de dissenyar les traces necessàries en base al Document del 'Pla de Seguretat i Traces' que posarà a disposició BIT 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.

5.19.9. Informe de seguretat

L'empresa proveïdora 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 a l'empresa proveïdora durant les primeres etapes del contracte.

5.20. Seguretat sistemes d'informació

En el present contracte s'utilitzen sistemes d'informació. Els sistemes d'informació són propietat de l'Ajuntament de Barcelona i el nivell de seguretat que cal aplicar als sistemes d'informació per part de l'empresa proveïdora és "Bàsic".