

Servei d'Arquitectura de Sistemes Oberts
Àrea alTec



Servei de suport a la publicació de serveis via API

Plec de Prescripcions Tècniques

Expedient número: **15012957**

Juliol 2024

Eduard Porquet Mateu
Resp. Arquitectura API

TAULA DE CONTINGUTS

1	Introducció	3
2	Àmbit.....	4
3	Tasques a desenvolupar	5
4	Modalitat de contractació.....	11
5	Especificacions tècniques	12
6	Característiques del servei	16

1 Introducció

1.1 Objectius del document i abast

L'objectiu d'aquest document és establir el plec de condicions de prescripcions tècniques complet per a la contractació dels treballs informàtics a realitzar per tal de complir amb l'objectiu del projecte que es descriu a continuació.

2 Àmbit

El present plec s'emmarca dins del servei d'Arquitectura de Sistemes Oberts, en la seva plataforma de publicació de serveis via API.

El servei que es pretén contractar és un servei informàtic que permeti **evolucionar** aquesta plataforma a nivell tecnològic per adaptar-se a les noves necessitats de la companyia.

3 Tasques a desenvolupar

Es pretén contractar la prestació d'un servei de suport en el manteniment i desenvolupament de petits evolutius de la publicació de serveis via API. Aquests inclouen tant la publicació com la securització dels serveis, i tot allò necessari per a la seva observabilitat i administració tècnica (automatitzacions, documentació...).

La realització de cada tasca pot requerir les següents tasques a fi de poder determinar el tipus de perfils requerits:

- Anàlisi funcional
- Disseny Arquitectura
- Implementació en codi
- Integració dins l'API
- Tests i Rendiment

A continuació es detallen alguns aspectes rellevants pel desenvolupament de les tasques.

3.1 Publicació de serveis

En la publicació de serveis hi ha diferents àmbits sobre els que donar suport i desenvolupar petits evolutius.

Primerament suport en els serveis de securització principals, que funcionen a dos nivells:

- **Autenticació:** identifiquen al client que fa la petició mitjançant unes claus (app keys), o bé amb un JWT via OIDC.
- **Autorització:** validen que els permisos (scopes) necessaris pel servei en qüestió estan assignats al client autenticat en el punt anterior.

També caldrà donar suport sobre el mecanisme que permet ajustar el contingut de la resposta en funció d'un rol assignat al client, amb els següents punts a tenir en compte:

- **Identificació de rols:** Identifica els rols que s'utilitzaran per gestionar els permisos i el control d'accés al servei REST. Cada rol representa un conjunt específic de permisos i privilegis.
- **Definició de permisos:** Enumera els permisos específics associats a cada rol. Aquests permisos determinaran quin contingut o funcionalitat pot ser accessible per cada rol.
- **Mapeig de permisos a endpoints:** Assigna els permisos definits als diferents endpoints del servei REST. Per a cada endpoint, indica quins rols tenen accés permès i quins no.
- **Validació de permisos:** En el moment de processar una sol·licitud al servei REST, valida els permisos del client en funció del rol assignat. Verifica si el rol del client té els permisos necessaris per accedir a l'endpoint i al contingut o la funcionalitat específica sol·licitada.
- **Tipus de permisos:** hi ha permisos de diferents tipus:
 - Per bloc: el permís restringeix o dona accés a tot un bloc de la resposta, en el cas del format JSON un atribut dins la estructura.

- Per contingut: el permís restringeix els continguts als objectes que compleixen un filtre o condició sobre el valor d'un atribut.
- **Ajust de contingut de la resposta**: Si el client té els permisos adequats, el servei REST ajusta el contingut de la resposta en funció del rol assignat. Això pot incloure mostrar o ocultar determinades dades, presentar informació addicional o restringir certes accions o operacions.
- **Gestió de errors i respostes no autoritzades**: Si un client intenta accedir a un endpoint o contingut per al qual no té permisos, el servei REST ha de gestionar adequadament aquesta situació. Podrà respondre amb un codi d'estat d'error i una resposta adequada, informant al client de la manca d'autorització per accedir a la funcionalitat sol·licitada, o bé directament amb un codi 403.
- **Proves i validació**: Davant una incidència, es realitzaran proves exhaustives per assegurar que els permisos es gestionen adequadament. Es verificarà que els clients amb rols diferents reben el contingut i les funcionalitats esperades i que els intents no autoritzats són bloquejats.

El servei inclou tractar incidències sobre qualsevol part d'aquest procés, i en cas de ser necessari, fer les adaptacions o petites evolucions que es vagin requerint per resoldre-les.

3.2 Consum dels serveis

Els aspectes rellevants a tenir en compte en la assignació i configuració dels permisos sobre un servei REST per un client són:

Definició dels rols i permisos: Identifica els rols necessaris per gestionar els permisos i defineix els permisos associats a cada rol. Això et permetrà establir qui té accés a quins recursos i quines accions estan autoritzades.

Configuració dels endpoints: Assigna els permisos requerits a cada endpoint del servei REST. Per cada endpoint, especifica quins rols tenen accés permès i quins no. Això s'ha de fer de manera granular per proporcionar un control precís sobre cada recurs.

Middleware d'autenticació i autorització: middleware en el servei de publicació que gestiona l'autenticació i l'autorització de les sol·licituds. Aquest middleware valida l'autenticitat del client i comprova si el rol del client té els permisos necessaris per accedir a l'endpoint sol·licitat.

La solució de configuració està basada en dades en format JSON però podrà evolucionar-se cap a models més avançats o basat en models relacionals, emmagatzemats en fitxers o base de dades.

La solució sempre ha de mantenir un enfocament "data-driven", la lògica del sistema ha de ser flexible i configurable a través de les dades de configuració, en lloc d'estar codificada directament en el codi de l'aplicació, permetent actualitzar la configuració sense necessitat de modificar el codi font de l'aplicació, afavorint la modularitat i facilitant la gestió del sistema.

A més, es podran dissenyar noves interfícies o modificar les existents eines de gestió per permetre als administradors modificar la configuració dels permisos de manera més senzilla i sense necessitat de tocar el codi de l'aplicació. Això pot ser a través d'un panell de control, una interfície web o eines de línia de

comandes que permetin actualitzar la configuració i aplicar els canvis sense interrompre el funcionament del sistema.

Amb aquesta solució es busca la flexibilitat, personalització i mantenibilitat del sistema, ja que els permisos i la seva configuració es poden adaptar fàcilment a mesura que les necessitats i els requeriments dels serveis evolucionen.

3.3 Manteniment del portal de desenvolupadors

Totes les anteriors funcionalitats, poden requerir d'ajustar tan visual com tècnicament l'actual portal de desenvolupadors. Es seguiran les línies de disseny de TMB, i en tot cas es podran demanar nous recursos o guies d'estil per nous components visuals que fossin necessaris.

3.3.1 Visualitzacions de detall

Pels casos de consulta d'una aplicació, caldrà mostrar visualment les dades més rellevants juntament amb dades de l'ús que està fent dels diferents serveis.

De la mateixa manera, des del punt de vista del responsable d'un servei (consulta per servei), caldrà mostrar la utilització del servei per part dels diferents clients.

Poden aparèixer noves necessitats que requerixen permetre editar alguna de les informacions associades a una aplicació o servei.

3.3.2 Nous serveis

Amb l'entrada de nous serveis a publicar a l'API, caldrà ajustar els continguts perquè siguin coherents amb l'aparició dels mateixos en els següents apartats:

- Documentació API (swagger)
- Exemples d'ús

4 Modalitat de contractació

La modalitat de contractació serà en format de bossa d'hores. La imputació de la mateixa es farà en base a les especificacions que TMB entregará al proveïdor i a la proposta de valoració que faci aquest. Si TMB accepta la valoració, es duran a terme les tasques i es farà un seguiment de la dedicació del proveïdor, que s'imputarà mensualment.

5 Especificacions tècniques

En aquest apartat es detallen les especificacions tècniques pels desenvolupaments de software.

5.1 Plataforma tecnològica

Es proposa seguir la següent pila tecnològica de components per la implementació de les diferents funcionalitats:

Component	Valor	Versió
Balanceig + Proxy	NGINX	Openresty 1.13.x
Llenguatge de programació i entorn d'execució.	JavaScript i NodeJS	ES5 / ES6 NodeJS 14.x
Autenticació / Autorització	AppID/AppKey OIDC	Openresty Keycloak 14.x
Publicació de serveis	Framework ExpressJS	4.x
Base de dades a memòria	Redis	5.x
Base de dades temps real	ElasticSearch	7.x
	ClickHouse	21.x
Serveis de mapes	GeoServer	2.19
	Vector Tiles Server	<i>latest</i>
Base de dades espacial	Oracle Spatial	19c
	PostGIS	9.6
Desplegament híbrid	Servidors Virtuals Cloud Públic	Windows 2016 / Linux RedHat 8 AWS Services
Clients Javascript	Bootstrap	BS 3.x / 4.x
	jQuery / React	<i>Latest</i>

	OpenLayers / Leaflet Mapbox GL	<i>OL 2.x-3.x / latest</i> <i>latest</i>
Gestió de codi font, tests, gestió de dependències, empaquetat o distribució,...	Github + npm Webpack	Latest

Taula 1 Entorn tecnològic**5.2 Entorns d'execució i desplegament: Arquitectura de servidors**

La plataforma està desplegada a infraestructura on-premise. S'automatitza el desplegament amb tasques d'Ansible, amb lo que tots els components han de tenir la capacitat de configurar-se externament (fitxers de configuració, variables d'entorn...).

També s'integren solucions externes en modalitat SaaS i parts de l'arquitectura poden utilitzar serveis al cloud (AWS principalment).

5.3 Integració amb API interna de TMB

Els serveis a desenvolupar han d'integrar-se sota l'API interna de TMB que requereix:

- Serveis RESTFul (sense estat)
- Format de les dades JSON / GeoJSON
- Integració amb seguretat d'API, segons el tipus d'autorització:
 - APP_ID/APP_KEY: cal suportar dos paràmetres extra (query GET), per validar si la crida es valida.
 - JSON WebToken: s'acceptaran un JSON WebToken a la capçalera de les crides, que es validarà si està signat correctament. En el contingut es podrà obtenir tant *scopes* com informació d'identificació del usuari que fa la crida, per fer l'autorització.
- Totes les comunicacions es realitzaran sobre el protocol HTTPS.

5.4 QA: Assegurament de la qualitat

Tots els lliuraments de software que es derivin del projecte hauran de passar els controls de qualitat que apliqui TMB. Hauran d'entregar-se mitjançant els sistemes de control de versions que ofereix TMB (SVN i Git).

No s'acceptarà cap lliurament sense aquest requeriment acomplert.

5.5 Entorn de desenvolupament i eines de QA

L'entorn de desenvolupament sobre el qual es realitzaran els treballs de construcció, proves, control de qualitat, documentació i col·laboració és el següent:

Funcionalitat	Producte/Servei
Entorn col·laboració	Redmine
Gestió de codi font	Git (Github)
Integració contínua	Jenkins
Repositori de versions de SW	AWS S3

Il·lustració 1 Entorn desenvolupament i QA

És obligatori l'ús d'aquestes eines durant l'execució del projecte.

5.6 Gestió de requeriments, bugs i noves funcionalitats

Caldrà gestionar els requeriments, bugs i noves funcionalitats mitjançant l'eina Redmine i GitHub. Aquesta gestió ha de ser continuada durant totes les fases del projecte. Sobretot en el cas de detectar funcionalitat que no queda clar si formen part de l'abast. Aquests temes es tractaran a les reunions de seguiment.

5.7 Nomenclàtors

TMB proporcionarà els nomenclàtors a fer servir per la codificació dels diferents components, tant pel llenguatge de programació com per la definició d'altres components.

5.8 Prohibicions

L'entorn de programació és l'anteriorment descrit, quedant explícitament prohibit la programació de components de SW fora d'aquest entorn, si no és prèviament analitzat i pactat amb TMB.

6 Característiques del servei

6.1 Lloc de realització dels treballs i horari

Els serveis objecte del contracte es prestaran des de les instal·lacions de l'adjudicatari.

En les ocasions que es requereixi d'un servei a les oficines de TMB es demanarà el desplaçament a l'adjudicatari amb una antelació mínima de 15 dies, sent obligació de l'adjudicatari l'aportació de les eines que siguin necessàries per a la prestació d'aquest servei. Es preveu una dedicació del 20% del temps a tasques desenvolupades a les oficines de TMB.

S'habilitarà a l'empresa adjudicatària un servei de connexió externa perquè puguin executar les tasques des de les seves oficines.

TMB disposa d'alguns llocs de treball a disposició de l'empresa adjudicatària.

6.2 Infraestructura i entorn tecnològic

TMB proporcionarà i determinarà la infraestructura i l'entorn tecnològic a usar durant el projecte.

6.3 Metodologia

L'adjudicatari dels serveis es compromet a seguir el marc metodològic de gestió de projectes TIC de TMB, actualment ITIL.

6.3.1 Seguiment i control

L'adjudicatari entregarà informes setmanals en format digital on es descriurà el grau d'avenç del projecte. En aquests informes s'hi inclourà, entre altres, els següents aspectes:

- Resum de les tasques realitzades durant la setmana
- Activitats previstes per la següent
- Riscos i desviacions
- Estat actual de la planificació

6.3.2 Estructura i nomenclatura dels lliuraments

L'adjudicatari haurà de seguir i respectar l'estructura i nomenclatura per tots els lliuraments, ja siguin documents o software, que proposi TMB.

6.3.3 Documentació

El nom dels documents seguirà un patró determinat, de manera que pugui identificar-se la següent informació respecte el document:

- Projecte
- Àmbit (Informe, Anàlisi, Disseny,...)
- Proveïdor, en el cas de les ofertes
- Nom descriptiu del contingut del document
- Extensió del fitxer Aquesta informació es compondrà formant un nom del fitxer de la següent manera:

PXXXXX. NomProjecte-ÀMBIT-PROVEÏDOR-Nom del Fitxer.ext Els valors del camp àmbit poden ser:

- **INFO:** Informe
- **ANA:** Anàlisi
- **DISS:** Disseny
- **PLEC:** Plec de condiciones
- **OFER:** Oferta,
- **MAN:** Manual
- **PRES:** Presentació
- **PLAN:** Planificació
- **PLA:** Pla de proves, pla de formació
- **ACT:** Acta
- **SEG:** Seguiment

La versió del document **NO** ha de formar part del mateix nom del fitxer ni del document, sinó que aquesta informació s'haurà de gestionar mitjançant l'apartat corresponent dins del document.

6.3.4 Entrega del servei

El projecte haurà de passar el conjunt de fases ITIL que componen la transició del servei.

Aquestes fases inclouen el lliurament del servei al departament d'operacions de l'àrea de tecnologia.

6.3.5 Lliuraments obligatoris

Es consideren lliuraments obligatoris els següents documents i arxius tècnics:

- Codi font generat
- Scripts de creació, inicialització i càrrega de base de dades
- Anàlisi funcional
- Model físic de base de dades
- Manual del desenvolupador
- Pla d'implantació
- Manual d'usuari
- Pla de proves funcionals

Qualsevol altra document generat en aquest projecte també serà lliurat.

6.3.6 Planificació

Tant la planificació, en durada i data d'inici, com la priorització es realitzarà conjuntament entre TMB i l'adjudicatari.

6.4 Seguretat i confidencialitat

6.4.1 Confidencialitat i publicitat del servei

L'adjudicatari està obligat a guardar secret respecte les dades o la informació prèvia que no essent públics o notoris estiguin relacionats amb l'objecte del contracte.

Qualsevol comunicat de premsa o d'inserció als mitjans de comunicació que el proveïdor realitzi referent al servei que presta a TMB l'haurà d'aprovar prèviament el client.

6.4.2 Propietat intel·lectual

TMB adquirirà en exclusiva la propietat intel·lectual de tot el material que sigui elaborat per l'adjudicatari en execució del contracte i en particular, de tots els drets de propietat intel·lectual patrimonial, industrial i d'imatge que derivin del mateix inclosa l'explotació en qualsevol modalitat i sota qualsevol format, per a tot el món, del treball elaborat per l'adjudicatari o els seus empleats en execució del contracte, reservant-se TMB qualsevol altra facultat annexa al dret de propietat intel·lectual o industrial.

Serà propietat de TMB el resultat dels serveis així quants materials i documents es realitzin en compliment del contracte.

TMB serà titular de tots els drets referits en el paràgraf anterior pel termini màxim legal permès i l'única organització que per tal concepte podrà explotar i comerciar amb el treball desenvolupat en execució del Contracte, abans o després del seu acabament, corresponent als autors materials del mateix únicament els drets morals que els reconeix la legislació vigent en matèria de propietat intel·lectual.

Als efectes previstos en els dos paràgrafs anteriors, l'adjudicatari es compromet al lliurament de tota la documentació funcional i tècnica, així com materials i lliuraments generats durant la prestació del servei i en el procés d'anàlisi, disseny, desenvolupament, implantació i proves de les mateixes. Tota la documentació elaborada i els resultats obtinguts per l'adjudicatari en execució del contracte seran propietat de TMB, en el poder del qual quedaran a l'acabament del contracte, no podent l'adjudicatari utilitzar-la per a altres persones, entitats o empreses.

L'adjudicatari respondrà de l'exercici pacífic de TMB en la utilització del programari i altres drets proporcionats per l'adjudicatari amb motiu del contracte i serà responsable de tota reclamació que pugui presentar un tercer per aquests conceptes contra TMB i haurà d'indemnitzar TMB per tots els danys i perjudicis que aquesta pugui sofrir per aquesta causa. En tot cas les relacions jurídiques derivades del contracte s'establiran entre TMB i l'adjudicatari. TMB no estarà contractualment vinculada amb persones diferents de l'adjudicatari.

6.4.3 Seguretat i protecció de dades

L'adjudicatari dels serveis es compromet a complir els requeriments de seguretat i de continuïtat aplicables a l'objecte del contracte especificats a:

- La legislació vigent en general i, en particular, quan es tractin dades de caràcter personal, a la informació de protecció de dades del QCAR genèric.

Adicionalment, l'adjudicatari es compromet a:

- Complir amb les directives tecnològiques, de seguretat i de qualitat que estableixi el client.
- Implementar les mesures, els processos, i els requeriments que el client sol·liciti amb aquesta finalitat i li proposarà els que consideri necessaris per millorar les solucions.
- Facilitat tota aquella informació que el client requereixi per tal que pugui donar compliment a la legislació i normativa referida en aquest apartat.

6.5 Compartició de recursos

Per motius de garantir la seguretat, qualsevol compartició de recursos tècnics (infraestructura, de maquinari, etc.) utilitzats en el marc de l'execució del contracte serà prèviament justificada al client amb un informe d'anàlisi de beneficis i de riscos, que aquest haurà d'aprovar.

Els adjudicataris utilitzaran la xarxa, el maquinari i/o el programari propietat de TMB exclusivament per a l'ús o el benefici de TMB.

6.6 Altres condicions

El conjunt d'eines utilitzades per l'adjudicatari per a la realització del projecte no ha d'implicar l'adquisició de llicències complementàries a les eventualment necessàries en manera operativa. TMB requereix una documentació de totes les eines utilitzades per al desenvolupament en format digital. A més, es requereix la producció i lliura de la documentació tècnica relativa a la implementació.

El lliurament de la plataforma completa es farà en l'entorn de desenvolupament de TMB. El traspàs a producció es realitzarà pel licitador, comptant amb el suport de TMB.

L'adjudicatari s'encarregarà de l'organització, realització i el seguiment de les proves necessàries, tant unitàries com funcionals que permetin garantir el correcte funcionament de tots els elements. Cada conjunt de proves haurà de comptar amb la documentació corresponent a l'escenari de proves i full de seguiment de les mateixes i amb la documentació corresponent al seguiment i correcció dels errors trobats durant el procés de proves.

L'idioma que es farà servir a l'aplicació (títols, missatges, ajuts, noms de camps, estructures, etc.) i a la documentació lliurada, serà el català.