Servei d'Arquitectura de Sistemes Oberts
Àrea aTec

Transports Metropolitans de Barcelona

Servei de Login B2B

Plec de Prescripcions Tècniques

Setembre 2025

Sergio Edo Arquero
Resp. Arquitectura GIS

TAULA DE CONTINGUTS

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 pel desenvolupament d'un sistema d'autenticació per a usuaris d'altres organitzacions autoritzades per TMB (B2B), que permeti l'accés segur i eficient als recursos corporatius. L'objectiu és garantir que només els usuaris autenticats i autoritzats puguin accedir als recursos, mitjançant la seva identitat corporativa (via email), i d'una forma integrada, dins la plataforma de login corporatiu de TMB.

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 Anàlisi funcional i requisits

La primera tasca serà definir l'abast i les condicions que ha de complir el servei de B2B login basat en un flux de Keycloak amb "magic link". El sistema ha d'implementar un flux d'autenticació basat en magic link integrat amb Keycloak: l'usuari introdueix el seu correu i, mitjançant l'enviament d'un enllaç temporal, s'inicia el procés d'autenticació. L'enllaç redirigeix al mecanisme d'autenticació i, abans d'atorgar credencials, dispara la validació per tenant. L'enllaç tindrà una validesa temporal i mesures per evitar re-utilitzacions malicioses; la mera recepció del link no comporta accés automàtic, sinó que actua com a iniciador de la comprovació d'autorització.

Per a cada tenant cal definir una regla o servei de validació que determini si l'usuari té dret d'accés. Aquesta validació s'ha d'exposar mitjançant una interfície única que Keycloak pugui invocar; el contracte d'entrada i sortida haurà d'estar clarament especificat (inputs, outputs, codis d'estat) i establir els temps màxims d'espera i comportaments en cas d'indisponibilitat. Les implementacions poden variar (crida al servei de la companyia, llistes blanques, validació del domini, etc.), però la interoperabilitat i la seguretat de les crides són requisits ineludibles.

El formulari d'accés ha d'admetre hints per permetre el pre-emplenament o l'evitació de camps obligatoris (email, organització) i, si cal, la selecció explícita del tenant des de la UI. Cal definir quins hints s'accepten, com es validen i escapen per prevenir injeccions i abusos, i establir controls anti-abusos (rate limits, captcha opcional) per protegir l'enviament massiu d'enllaços.

Després de la validació, s'ha de definir el cicle de vida de les identitats i les sessions: la creació temporal d'un usuari en el tenant (si s'escau), la durada de la sessió, l'ús i caducitat de refresh tokens i els mecanismes de revocació. També s'ha d'establir la política d'impacte sobre sessions actives en cas de revocació o modificació de permisos per garantir coherència entre autorització i sessions en curs.

El servei ha de proporcionar traçabilitat completa: registre d'enviaments d'enllaços, invocacions de validació per tenant, resultats (acceptat/denegat) i emissió de tokens, amb metadades mínimes (tenant, IP d'origen, user agent, timestamp). Cal definir polítiques de conservació, accés i consulta per a finalitats d'auditoria i compliment normatiu.

Finalment, s'ha d'establir el comportament davant d'errors i mecanismes de fallback: respostes estandarditzades per a indisponibilitat de la validació, timeouts o errors externs, i criteris UX per mostrar missatges clars a l'usuari i opcions de reintent. També cal definir el procés d'onboarding i configuració de tenants, incloent la parametrització de la metodologia de validació triada, la definició de contactes operatius i les proves de validació prèvies a l'entrada en producció.

3.2 Disseny de la solució

La seguretat del servei ha de contemplar controls específics per evitar l'ús maliciós dels magic links. Això inclou una validesa temporal curta, ús únic (single-use) i mesures addicionals opcionalment vinculades a l'origen (binding per IP o user-agent) segons el nivell de risc del tenant. Totes les crides i enllaços han d'anar sempre sobre TLS; la signatura dels tokens i dels enllaços ha de ser verificable i la gestió de secrets ha de complir bons pràctiques (rotació, accés restringit, custòdia segura). On correspongui, el servei ha d'ajustar-se als requisits de seguretat (ENA nivell Mitjà).

La robustesa del servei de validació per tenant és crítica: la validació ha de respondre dins d'un llindar predefinit (per exemple < 500 ms) o disposar de mecanismes de degradació que garanteixin un comportament segur en cas d'indisponibilitat. Cal definir SLAs per a les invocacions de validació, polítiques de reintents i criteris de fallback per assegurar la continuïtat del flux sense comprometre la seguretat.

Pel que fa a la privacitat, el sistema només ha d'enviar i emmagatzemar les dades estrictament necessàries per a la validació (p. ex. email, identificador de tenant i metadades d'auditoria). S'han de documentar i aplicar períodes de conservació de dades i procediments clars d'eliminació d'enllaços obsolets i logs, així com controls d'accés per protegir la informació personal segons la normativa vigent.

En termes de rendiment, el servei ha de poder gestionar pics d'enviament d'enllaços (per exemple en llançaments o pilots massius). Cal establir objectius mesurables (latència p90 per emissió d'enllaç i per validació) i estimacions de volum (verificacions per minut en hora punta) que serviran com a criteris d'acceptació en les proves de càrrega.

L'observabilitat i la seguretat operativa són requisits imprescindibles: el sistema ha d'incorporar detecció d'anomalies (enviaments massius, intents repetits des de la mateixa IP), alertes operatives i dashboards per a monitoratge. Els logs han

de ser estructurats i suficientment detallats per facilitar investigacions i proofs d'auditoria sense exposar dades sensibles.

Finalment, la mantenibilitat exigeix que la interfície d'invocació de validació per tenant sigui estable i versionada, garantint compatibilitat enrere per permetre implementacions diferents per tenant sense afectar el flux central. Això inclou polítiques de versionat, documentació de contractes i un pla de migració per actualitzacions del contracte API.

3.3 Integració de les autoritzacions

L'interfície de autorització per tenant s'ha de definir com una API genèrica i versionada amb contracte OpenAPI clar. El contracte ha d'establir inputs obligatoris (email, tenant, hints, metadata), outputs previstos (accept, deny, reason, attributes) i codis d'estat, així com els temps màxims d'espera i criteris de reintents. Les crides hauran d'estar autenticades i xifrades, i caldrà especificar el comportament en cas d'indisponibilitat per garantir una degradació segura del flux d'autenticació.

Els proveïdors d'autorització per tenant poden implementar diferents estratègies (API pròpia de la companyia, llistes blanques, validació de domini, consultes a bases de dades internes). Per a cada estratègia caldrà definir el mecanisme d'autenticació i autorització, els formats d'entrada/sortida i les garanties de seguretat (TLS, certificat o token). També s'han d'establir polítiques de timeout, reintents i fallback per garantir continuïtat en cas de fallada del proveïdor.

El servei d'enviament d'emails ha de proporcionar idempotència i mecanismes per rastrejar l'estat dels enllaços (emès, entregat, clicat, caducat). S'hauran d'acordar plantilles per tenant, límits d'enviament, garanties de lliurament i procediments per gestionar rebots i bloquejos. L'integrador garantirà que els enllaços siguin signats i verificables i que el servei compleixi polítiques de privacitat i retenció de dades.

La integració amb Keycloak requereix definir el punt d'extensió (SPI/extension) que invocarà l'API d'autorització i el comportament segons la resposta (accept/deny). Cal documentar personalitzacions, limitacions d'upgrade i responsabilitats entre TMB i el proveïdor pel manteniment i actualitzacions. També s'ha d'acordar el model de tokens i claims que Keycloak emetrà un cop validat l'accés.

La captura i ingestió d'esdeveniments al sistema corporatiu de logs és obligatòria per a auditoria i monitoratge. S'ha d'establir el catàleg d'esdeveniments mínims (emissió d'enllaç, validacions, emissions de token, errors crítics), el format dels

logs, la retenció i les regles d'accés, així com alertes i dashboards per a detecció d'anomalies.

La UI/formulari d'accés exposarà els hints per al pre-emplenament i la selecció de tenant, però sempre validarà i escaparà aquestes dades en servidor. S'hauran d'acordar els camps acceptats, les regles de validació, controls anti-abusos (rate limits, captcha opcional) i les normes d'usabilitat i accessibilitat. Finalment, caldrà definir el contracte de seguretat entre UI i backend per protegir el flux d'enviament d'enllaços i les dades sensibles.

3.4 Desenvolupament backend i APIs

El desenvolupament backend ha d'entregar APIs RESTful estables i contractades que implementin el flux d'emissió d'enllaços, la invocació de la validació per tenant i la gestió del cicle de vida d'identitats i sessions. Les APIs han d'estar descrites amb OpenAPI i incloure definicions clares d'inputs obligatoris, outputs, codis d'error i comportaments en cas d'indisponibilitat. Cal garantir idempotència en les operacions d'emissió d'enllaç i capacitat per auditar cada petició amb metadades mínimes (tenant, email, origen, timestamp).

S'ha d'implementar el middleware OIDC/Keycloak necessari per integrar el flow de magic link: un punt d'extensió (SPI) que invoqui la interfície de validació, gestioni la creació temporal d'usuari si escau i decideixi l'emissió de tokens amb els claims corresponents. Les personalitzacions sobre Keycloak s'han d'implementar com a extensions documentades i versionades, evitant canvis al core que impedeixin upgrades.

Les dependències infra (Redis, Elastic, Kafka) s'utilitzaran per funcions concretes: Redis per idempotència, rate limiting i cache de sessions/estat temporal; Kafka per registrar esdeveniments i processos asíncrons relacionats amb l'onboarding i la sincronització; Elastic (o similar) per indexar logs i proporcionar cerca/consultes d'auditoria. El disseny ha d'aclarir les garanties de consistència i les polítiques de fallback quan algun component estigui degradat.

La qualitat del codi es garantirà amb cobertura de tests unitaris, proves d'integració amb simulació dels serveis externs i contract tests per la API de validació per tenant. Les proves automàtiques s'executaran en CI; s'estableix un llindar de cobertura mínim (indicatiu, ex. 70–80%) i criteris d'acceptació per a proves de càrrega i latència (vegeu NFRs). També s'han de lliurar runbooks per a desplegament i rollback, i documentació tècnica de les APIs, extensions de Keycloak i esquemes d'esdeveniments per a ingestió en SIEM.

Entregables mínims:

- Especificació OpenAPI de totes les APIs exposades.

- Codi de les extensions Keycloak (SPI) amb README d'integració.
- Tests automatitzats: unitaris, d'integració i contract tests.
- Scripts/Playbooks per desplegament i rollback.
- Document d'operacions: runbooks, llistat de mètriques i alertes.
- Plan de proves de càrrega amb criteris d'acceptació.

Criteris d'acceptació bàsics:

- OpenAPI validada i acordada amb equips integradors.
- Passen tots els tests automàtics en CI.
- Latències i comportaments en proves de càrrega dins dels límits establerts.
- Logs i events arriben al sistema de logs amb l'esquema acordat.

3.5 Desenvolupament frontend i UX

El frontend ha de proporcionar una experiència clara i segura per a l'enviament i recepció de magic links. El formulari d'accés ha de ser intuïtiu, responsiu i accessible (compliment WCAG 2.1 AA), permetent l'entrada d'email i la selecció o pre-selecció del tenant via hints. La interfície ha de validar i escapar totes les dades d'entrada en client i servidor, i oferir missatges d'error i èxit comprensibles i orientats a l'operativa de l'usuari (reintents, gestió d'enllaços caducats, comprovació d'entrega).

S'han de dissenyar els fluxos principals i les variacions d'error: sol·licitud d'enllaç, confirmació d'enviament, enllaç caducat, reemissió i ajuda/autogestió. El flux de reemissió ha de contemplar controls anti-abusos (rate limiting, captchas opcionals) i mecanismes per que l'usuari pugui iniciar la resolució d'incidències (contactes operatius). Els textos i plantilles d'email han de ser coherents per tenant i susceptibles de personalització sense trencar la seguretat dels enllaços.

Els prototips (wireframes i mockups interactius) s'han de lliurar en fase inicial per validar usabilitat amb stakeholders i amb una prova pilot amb usuaris representatius. Les proves d'usabilitat han d'avaluar temps de completat, taxa d'èxit i incidències crítiques; els resultats han de generar una llista d'accions correctores abans de l'obertura del pilot.

Consideracions d'accessibilitat i internacionalització:

- Textos i missatges en català per defecte; preparar fitxers de traducció.
- Suport per navegadors i dispositius mòbils habituals.
- Controls d'accessibilitat (navegació per teclat, etiquetatge ARIA, contrast).
- Entregables mínims:

Prototips interactius i mockups validats.

- Guia d'estil i textos d'UX per a totes les pantalles i emails.
- Pla de proves d'usabilitat amb resultats i conclusions.
- Implementació frontend amb tests d'acceptació automatitzats (E2E).

Criteris d'acceptació bàsics:

- Tasques clau completes per usuaris pilot amb èxit ≥90%.
- Compliment d'accessibilitat WCAG 2.1 AA per pantalles crítiques.
- Missatges d'error i recuperació clars i validats en proves.
- Integració segura amb backend (HTTPS, validació d'inputs, escapes).

3.6 Proves i validació

L'estratègia de proves cobreix totes les fases del cicle de vida del software per garantir la qualitat, la seguretat i el compliment dels lliuraments abans del pilot i la posada en producció. Cal organitzar plans de proves separats però traçables: proves unitàries que validin la lògica de cada mòdul; proves d'integració que verifiquin contractes entre components (per exemple OpenAPI vs. implementació de la interfície de validació per tenant); proves end-to-end que recorreguin el flux complet de magic-link des del formulari fins a l'emissió de token; proves de regressió automàtiques per assegurar que canvis futurs no trenquin funcionalitats existents; proves de càrrega i rendiment per validar latències p90 i capacitat en pics; i pentesting (extern) per validar resiliència davant vectors d'atac rellevants.

Cada tipus de prova ha d'incloure: objectiu, criteris d'entrada, casos i dades de prova, criteris d'acceptació i responsabilitats. Les proves d'integració i contract tests han d'incloure simulacions dels proveïdors de validació per tenant (stubs/mocks) i tests de tolerància a latències/erros externs. Les proves de càrrega han d'establir escenaris representatius (emissió massiva d'enllaços, validacions concurrents) i mesurar pèrdues, temps de resposta i degradació segura.

Els resultats han d'estar documentats amb evidències (logs, traces, informes de càrrega i vulnerabilitat) i amb un pla d'acció per a les incidències trobades. Els criteris d'acceptació generals per passar a pilot/producció inclouen: tots els requisits funcionals prioritaris amb proves superades; absència de vulnerabilitats crítiques; i cobertura mínima de tests automatitzats acordada (indicativa 70–80%). S'han de lliurar fulls de proves, scripts d'execució CI, informes de càrrega i informe de seguretat.

3.7 Documentació, formació i transferència de coneixement

La documentació ha de permetre l'operació, manteniment i evolució del servei per part dels equips de TMB i dels operadors assignats. Cal lliurar manuals tècnics que expliquin l'arquitectura, comportaments esperats, diagrames de flux i decisions clau (ADR); documentació d'API (OpenAPI complet i exemples d'ús); guies d'integració i contract tests; i especificacions d'esdeveniments/logs per la ingestió al sistema de logs.

Per a l'operativa, s'han d'entregar playbooks amb procediments de desplegament, rollback, recuperació d'incidents i operacions rutinàries (onboarding de tenants, reemissió d'enllaços, revocació massiva). La documentació d'operacions inclou requisits de monitoratge, llistat de mètriques i thresholds d'alerta, i instruccions per a l'accés a logs i traçabilitat per a auditoria.

La transferència de coneixement ha d'incloure sessions de formació pràctica per a equips operatius i administradors (workshops i demos), materials de suport (presentacions, FAQ, vídeos curts) i una sessió de formació per a desenvolupadors integradors que cobreixi el contracte OpenAPI i exemples de proves. També cal provar la transferència amb una sessió de validació en la qual els equips de TMB executin tasques clau guiats per l'adjudicatari.

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 entregarà 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 ClickHouse	7.x 21.x
Serveis de mapes	GeoServer Vector Tiles Server	2.19 *latest*
Base de dades espaial	Oracle Spatial PostGIS	19c 9.6
Desplegament híbrid	Servidors Virtuals Cloud Públic	Windows 2016 / Linux RedHat 8 AWS Services
Clients Javascript	Bootstrap jQuery / React	BS 3.x / 4.x *Latest*

	OpenLayers / Leaflet Mapbox GL	*OL 2.x-3.x / latest* *latest*
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, Anàlisis, Disseny,..)
- Proveïdor, en el cas de les ofertes
- Nom descriptiu del contingut del document
- Extensió del fitxer Aquesta informació es composarà 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*: Anàlisis
  - *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 composen 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
- Anàlisis 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.

Addicionalment, 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'anàlisis 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.

7 Criteris ambientals

7.1 Impressió d'informes - documents de treball i/o documents finals

En cas que sigui necessària la impressió de qualsevol document de treball, s'haurà de:

- Acordar amb TMB la impressió o no del mateix. I prioritzar:
    - Reduir el màxim possible el número de impressions, ajustant-les a les necessitats.
    - Utilitzar paper 100% reciclat (excepte per plànols no imprimibles en DINA4 o DINA3).
    - Imprimir els documents a doble cara i en blanc i negre (el color només s'utilitzarà en casos en els que no es pugui interpretar en blanc i negre)

7.2 EMBALATGES - no primaris material reciclat

En el cas que la licitació inclogui el lliurament de productes o materials, i aquests se subministrin amb embalatges no primaris, aquests hauran d'estar fabricats íntegrament amb materials reciclats.

(*) embalatge addicional al del propi material per a la distribució final del producte)