

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA CONTRACTACIÓ DEL SERVEI D'ALLOTJAMENT DEL SITMUN I LA IDEBARCELONA

Índex de continguts

1. Objecte.....	1
2. Descripció general	1
3. Descripció del servei	3
4. Administració i operació del servei.....	6
5. Comunicacions	11
6. Migració de la plataforma entre empreses de <i>hosting</i>	11
7. Equip de treball tècnic	13
8. Seguretat i qualitat	13
9. Responsabilitat del servei.....	15
10. Contingut i estructura de les ofertes tècniques	15

1. Objecte

És objecte del present plec fixar les condicions tècniques a les quals s'ajustarà el procediment per a la contractació del servei d'allotjament del Sistema d'Informació Territorial Municipal (SITMUN) i la Infraestructura de Dades Espacials de la Diputació de Barcelona (IDEBARCELONA), amb garanties de disponibilitat, continuïtat i escalabilitat.

2. Descripció general

La Diputació de Barcelona (DIBA), a través de l'Oficina Tècnica de Cartografia i SIG Local (OTCSL), disposa d'una Infraestructura de Dades Espacials des de la qual s'ofereixen diversos serveis, eines i recursos al món local, a la ciutadania i també a nivell intern, en l'àmbit de la informació geogràfica i la gestió del territori. Entre aquests recursos hi ha els que ofereix la plataforma SITMUN (Sistema d'Informació Territorial Municipal) i la IDEBARCELONA (Infraestructura de Dades Espacials de la Diputació de Barcelona). Aquesta plataforma posa a disposició dels usuaris (externs, interns, administradors i ciutadans) eines que faciliten tant la gestió de la informació geogràfica com la seva integració, publicació i distribució, així com el compliment de les normatives aplicables.

Per oferir aquest servei és necessària una infraestructura informàtica on els servidors i les connexions són l'eix central del sistema, donat que es troben contínuament en funcionament. Cal, doncs, protegir especialment els seus accessos físics, així com garantir les condicions ambientals en les quals aquests components han de funcionar. Per aquest motiu, cal que els servidors estiguin ubicats en un Centre de Processament de Dades (CPD). Un CPD és un centre degudament protegit i dissenyat per treballar en unes condicions ambientals determinades (temperatura, humitat, altitud, interferències electromagnètiques, vibracions,...). Entre les mesures de control ambiental de què ha de disposar el CPD destaquen els sistemes contra incendis i inundacions, els sistemes de control de temperatura i el sistema d'alimentació ininterrompuda. A més, cal que el CPD estigui equipat adequadament a nivell de programari per assegurar una protecció completa de ciberseguretat. Aquest aspecte és clau i indispensable.

L'empresa adjudicatària s'ha d'encarregar de proveir els serveis necessaris per satisfer les condicions tècniques de la plataforma informàtica que es detallen en aquest plec.

El contracte inclou els següents serveis:

- Servidors: Servidors virtuals i llicències de programari de base (sistemes operatius i d'escriptori remot). Inclou la instal·lació, configuració, actualització i manteniment del conjunt, de forma proactiva i també a petició de l'OTCSL però sempre de manera acordada amb l'OTCSL.
- Seguretat: Tot el necessari per garantir la confidencialitat, integritat, disponibilitat i protecció contra ciberatacs de la informació allotjada als servidors. Propostes de millores en aquest sentit, de manera proactiva.
- Còpies de seguretat: Pla detallat de custòdia de dispositius i polítiques de còpia de seguretat per a cada servidor.
- Comunicacions: Infraestructura de comunicacions robusta i redundada per garantir la continuïtat dels accessos entre el CPD i internet, i entre el CPD i el personal autoritzat de l'OTCSL.
- Monitorització i explotació dels sistemes, amb una gestió d'alertes que permetin garantir la disponibilitat dels sistemes. Aquesta gestió ha d'incloure la seva notificació en temps real a l'OTCSL, així com la seva resolució amb el mínim de temps segons el que s'estableixi.
- Serveis professionals per a la resolució d'incidències
- Serveis professionals d'operació remota 24x7 dels sistemes implicats i la infraestructura tecnològica associada.
- Serveis professionals per a la gestió de còpies de seguretat i recuperació de les dades totals i parcials.
- Serveis professionals per garantir la continuïtat del servei en cas de fallada del CPD.
- Serveis professionals per a la instal·lació de nous programaris, noves versions i instal·lació/actualització de versions de les bases de dades.
- Actuacions als servidors a petició de l'OTCSL: els tècnics de l'OTCSL no disposen de tots els permisos d'administració sobre els servidors, pel qual certes accions les ha d'executar l'equip tècnic de l'adjudicatari a petició de l'OTCSL.
- Un mínim de 15 connexions concurrents i per dispositiu als servidors del CPD (via VPN i RDP) per al personal tècnic de l'OTCSL i per a tercers que hi requereixin accés, independentment de la IP des d'on es fa la connexió, per assegurar el teletreball i amb totes les mesures de seguretat que es requereixin. Si es detecta que l'accés es fa des d'una IP

fora d'Espanya, es notifica el fet a l'OTCSL El contractista es responsabilitza de controlar que no s'excedeixi el nombre màxim de connexions contractades.

- Mesures de control ambiental. El CPD ha de disposar de mesures de control ambiental, entre les que destaquen els sistemes contra incendis i inundacions (extintors, portes ignífugues, drenatges i vies d'evacuació), els sistemes de control de temperatura (no s'han de superar els 30º) i un sistema d'alimentació ininterrompuda.
- Serveis professionals per al tractament adequat i d'urgència en cas d'un possible ciberatac.

3. Descripció del servei

3.1 Configuració actual dels servidors

Actualment l'OTCSL té contractada una plataforma informàtica a una empresa de *hosting*, que inclou els servidors que es descriuen a continuació, virtualitzats amb el programari VMware.

Per al correcte funcionament de la plataforma SITMUN es disposa de quatre servidors, ubicats en un *Data Center* amb garanties de funcionament durant les 24 hores del dia i tots els dies de la setmana. Dels quatre servidors, n'hi ha dos per a l'entorn de Producció (servidor d'aplicacions i servidor de dades) i dos per a l'entorn de Pre-producció.

Un cop adjudicat el contracte es lliurarà a l'empresa un document detallat de la configuració actual dels servidors.

Notació utilitzada al present plec:

- “S1”: servidor web i d'aplicacions (front-end) de l'entorn de Producció
- “S2”: servidor de bases de dades (back-end) de l'entorn de Producció
- “S3”: servidor web i d'aplicacions (front-end) de l'entorn de Pre-producció
- “S4”: servidor de bases de dades (back-end) de l'entorn de Pre-producció

3.1.1 Característiques comunes dels quatre servidors (S1, S2, S3, S4)

- El servidor de llicències de Terminal Server està al servidor S1
- Accés via escriptori remot (RDS)
- Visibilitat entre els servidors S1-S2 i entre S3-S4 per possibilitar la còpia de fitxers
- Virtualització VMware
- Informació redundada per a S1 i S2 per a assegurar l'alta disponibilitat

3.1.2 Servidors web/aplicacions: S1 (Producció) - S3 (Pre-producció)

Sistema operatiu Windows Server 2019 Standard i un conjunt d'aplicacions i serveis instal·lats, entre els quals es destaquen:

- Aplicacions a mida i també comercials que s'executen sota Tomcat (Apache).
- Aplicacions a mida i també de codi obert que s'executen en Docker
- Utilitats d'IIS com FTP, correu, control de redireccions, tractament de logs,...
- Aplicacions a mida que s'executen des de wwwroot\inetpub.
- Aplicacions client d'Oracle.
- Tasques programades amb Task Scheduler.

- Entorn Java.
- Aplicacions específiques de SIG, com QGis, Gaia, aplicacions comercials, etc.

En el cas del servidor S3, cal destacar que disposa d'entorns/eines relacionades amb el desenvolupament d'aplicacions, com Eclipse, node.js, git, Visual Studio Code, etc.

3.1.3 Servidors de dades: S2 (Producció) – S4 (Pre-producció)

Sistema operatiu Windows Server 2019 Datacenter i base de dades Oracle amb l'opció Locator, a més d'un conjunt d'aplicacions i serveis instal·lats: aplicacions a mida i també comercials, com FME i aplicacions d'Oracle..

3.1.4 Funcionament actual de les llicències per escriptori remot

Els quatre servidors permeten fins a 10 sessions úniques i disposa d'una gestió apropiada per al control de sessions desconnectades per evitar sessions de durada infinita.

3.1.5 Configuració actual de les còpies de seguretat o backups

S'estan realitzant diferents nivells de backups de tots els servidors, que queden emmagatzemats en un segon datacenter. Concretament:

- Diari: retenció de 7 dies i ubicat a un altre datacenter
- Setmanal: retenció d'1 mes (4 punts de backup)
- Mensual: retenció de 12 mesos

A més, s'estan generant rèpliques per a recuperació en cas de desastre únicament per als servidors de PRO (S1 i S2). Concretament, es fa una rèplica cada 24 hores a uns servidors ubicats al segon datacenter

Pel que fa a la base de dades, també es fan diversos tipus de backup diari:

- PRO (S2): físic i lògic
- PRE (S4): lògic

3.2 Configuració dels nous servidors

A continuació es descriu la configuració desitjada per als nous servidors, que han de ser virtuals.

3.2.1 Requisits mínims fixats inicialment

- Inicialment es requereixen 4 servidors amb sistema operatiu Windows Server 2019 Datacenter:
 - S1: servidor web/aplicacions entorn de Producció (Windows)
 - S2: servidor bases de dades entorn de Producció (Windows)
 - S3: servidor web/aplicacions entorn de Pre-producció (Windows)
 - S4: servidor bases de dades entorn de Pre-producció (Windows)

Cal preveure la possibilitat de que en algun moment del contracte es requereixin 1 o 2 servidors addicionals, sense cost de llicència de sistema operatiu i amb un mínim de disc, memòria i CPU obtinguts per redistribució dels recursos disponibles.

- Els discos hauran de ser de tipus SSD. Es preveu no assignar tot l'espai en iniciar cada un dels anys del contracte i, a mesura que sigui necessari, assignar més espai al servidor que ho requereixi en el moment que es necessiti, sempre dins del límit de disc definit per aquell any. A l'iniciar el contracte s'indicarà el repartiment inicial d'una part de l'espai de disc per cada un dels servidors.
- En total es requereix un mínim de 320 Gb de memòria RAM. Haurà de ser de tipus DDR5. Es preveu re-assignar memòria RAM entre els servidors a mesura que sigui necessari, en el moment del contracte que es necessiti. A l'iniciar el contracte s'indicarà el repartiment inicial de memòria RAM per a cada un dels servidors.
- En referència a la CPU, es requereix un mínim de 20 vcpu en total. Hauran de ser d'última generació (mínim de tipus 45). Es preveu re-assignar vcpu entre els servidors (d'un servidor a un altre) a mesura que sigui necessari. A l'iniciar el contracte s'indicarà el repartiment inicial de les vcpu per a cada un dels servidors.
- Connexió concurrent (via VPN i RDP) amb un mínim de 15 dispositius connectats. Cal establir un mecanisme que permeti l'execució desatesa de sessions llargues en remot però a la vegada faciliti el tancament de sessions que no s'usen, sempre tenint molt present que cal vetllar per la seguretat. Ha d'estar disponible per tots els servidors, cadascun amb el protocol que es consideri més adient i s'acordi amb l'OTCSL.
- Les llicències per als sistemes operatius Windows i les d'escriptori remot han de ser proporcionades per l'empresa adjudicatària, i han d'estar incloses en aquest contracte.
- Caldrà instal·lar aplicacions en Docker en aquesta plataforma, pel que es requereix que l'empresa adjudicatària tingui els coneixements necessaris per poder administrar/gestionar servidors amb Docker sobre Windows (amb WSL2 o similar), així com que disposi de les eines adients per a fer aquesta administració (Docker, Docker compose, Docker Desktop, etc.).
- Els servidors S2 i S4 tindran instal·lada una base de dades Oracle SE2. Cal tenir en compte que es disposa de dues llicències, una per a cada servidor per a un màxim dos processadors cada una, que és el límit que estableix l'Oracle Standard 2 (SE2). Serà responsabilitat de l'adjudicatari dimensionar els servidors S2 i S4 per complir amb els requeriments de llicenciament del fabricant Oracle. En el cas d'incompliment serà responsabilitat de l'adjudicatari la regularització de les llicències necessàries, sense cost addicional per a la DIBA. Cal preveure la possibilitat que durant el període del contracte s'afegeixi una o més bases de dades PostgreSQL amb Postgis a la plataforma (sense cost de llicència).
- Pel que fa al programari, cal tenir en compte que les versions indicades al present plec i al document de configuracions que s'entregarà a l'adjudicatari són orientatives, essent possible proposar versions superiors. El procés d'actualització de versions de tots els programaris instal·lats als servidors és responsabilitat de l'adjudicatari durant tot el període de vigència del contracte. També serà responsabilitat de l'adjudicatari la instal·lació de nous programaris

que es puguin requerir durant el mateix període. En qualsevol cas, cal assegurar la compatibilitat entre ells. Totes les instal·lacions cal fer-les sense cost addicional per a la DIBA.

- L'empresa adjudicatària proporcionarà el programari necessari per a la prestació del servei com els relacionats amb la seguretat, antivirus i *malware*, còpies de seguretat, monitorització, generació d'informes i estadístiques.

3.2.2 Requisits variables

Està previst que durant el contracte es requereixi ampliar l'emmagatzematge i distribució dels següents productes:

- Ortofotos
- Models digitals/elevacions (terreny, superfícies, ombres, orientacions, pendents)

És per aquest motiu que l'espai mínim de disc requerit a la plataforma és variable i incremental en el temps. I més concretament, es preveu que s'incrementarà la necessitat d'espai de disc anualment, també en cas de pròrroga del contracte, segons el que es detalla a continuació. Inicialment es requereixen 3 Tb amb un creixement anual de 3 Tb / any, és a dir:

- Any 1: 3 Tb
- Any 2: 6 Tb
- Any 3: 9 Tb
- Any 4: 12 Tb

3.3 Ubicació dels CPD

Els dos CPD necessaris per al servei (principal i secundari) han d'estar ubicats dins l'àmbit territorial de l'Espai Econòmic Europeu (EEE), no permetent-se cap comunicació fora d'aquest territori, per tal de garantir la protecció de dades segons la normativa europea.

A més, als efectes de minimitzar els costos derivats dels desplaçaments dels tècnics de la Diputació per a la visita inicial de les instal·lacions i de totes les que siguin necessàries durant la vigència del contracte, un dels dos CPD haurà d'estar ubicat a una distància màxima de 200 km de Barcelona ciutat.

Als efectes de seguretat, els CPD principal i secundari cal que es trobin a una distància mínima entre ells, de manera que el CPD secundari pugui passar a funcionar com a principal en cas de desastre a les instal·lacions del CPD principal.

4. Administració i operació del servei

Serà competència de l'adjudicatari l'administració i configuració del programari instal·lat als servidors. També donarà suport a l'administració de les bases de dades geoespacials.

La realització de tasques programades en el CPD, tant de manteniment d'instal·lacions, com de manteniment i actualització d'equips i sistemes informàtics i de comunicacions, no afectarà a la prestació del servei.

4.1 Actualització de versions / Nou programari

D'acord amb el personal tècnic del CPD i l'OTCSL, es programaran les actualitzacions i/o pedaços del programari instal·lat, així com la instal·lació de nou programari que es requereixi, sempre assegurant la compatibilitat amb la resta de programari instal·lat.

Pel que fa a les actualitzacions que solucionen errors i vulnerabilitats o milloren el funcionament del programari, caldrà establir un protocol d'actuació per part del personal tècnic del CPD. Aquest haurà de proposar els pedaços o actualitzacions de manera proactiva, fent èmfasi als que corregeixin possibles problemes de vulnerabilitat, i instal·lar-los, sempre d'acord amb l'OTCSL, qui haurà de donar el vistiplau. L'objectiu és aplicar les actualitzacions imprescindibles per al correcte funcionament de la plataforma.

En el cas de nou programari o canvi de versió, caldrà elaborar una matriu de compatibilitat dels programaris instal·lats, per assegurar el correcte funcionament de la plataforma. També haurà de ser possible realitzar un *snapshot* de servidor just abans de fer la instal·lació, que permeti retornar a l'estat anterior de la instància, si es requereix. Aquest *snapshot* caldrà mantenir-lo un mínim de 15 dies.

També s'actualitzaran els certificats dels servidors.

L'empresa controlarà les versions del programari instal·lat a cada servidor i els fitxers de configuració associats a cada programari.

En qualsevol cas, les instal·lacions de programari es faran sempre d'acord amb l'OTCSL.

4.2 Còpies de seguretat

Serà necessari aplicar tots els mecanismes que es considerin adients per a la protecció de la informació. Un dels que caldrà aplicar consisteix a realitzar les còpies de seguretat necessàries que hauran de ser utilitzades en cas d'haver de restaurar la informació al punt que permeti que un servei o sistema pugui tornar a estar operatiu, o en cas que interessi tornar a un punt anterior de l'estat de la informació, sempre assegurant la mínima pèrdua de dades possible segons la política de còpies de seguretat que s'acordarà a l'inici del contracte amb l'OTCSL.

Per als servidors de producció, és necessari implantar un servei de protecció addicional que garanteixi la possibilitat de recuperar l'estat de les màquines virtuals a un punt del temps. Això s'implementarà mitjançant un sistema d'*snapshots* immutables, amb punts de restauració de mínim cada 2 hores i que es guardin durant un total de 48 hores, de manera que sempre es disposi de 24 imatges per a una possible necessitat de restauració. Aquests *snapshots* immutables han d'estar protegits de manera que no es poden eliminar, encriptar ni modificar. La seva protecció i la de qualsevol tipus d'eliminació o modificació dels temps de caducitat ha d'estar basada en la validació de dos o més contactes diferents autoritzats, i executat pel suport tècnic del fabricant.

S'ha de garantir la mateixa seguretat (integritat, confidencialitat, autenticitat i traçabilitat) a les còpies que a les dades originals. A més, per tal que sigui possible la continuïtat del servei, cal que les còpies estiguin duplicades com a mínim en un CPD secundari, el qual ha de tenir la possibilitat de recuperació en cas d'un desastre que afecti al CPD principal.

S'especificarà el lloc on s'emmagatzemaran les còpies, que ha de ser en una altra ubicació física.

S'acordarà amb l'OTCSL i s'aplicarà una política de còpies que com a mínim englobi les que s'estan realitzant actualment, descrites en l'apartat "Configuració actual de les còpies de seguretat o backups" del present plec. A més, caldrà aplicar-ho de forma anàloga als possibles nous servidors no contemplats en l'esmentat apartat.

L'adjudicatari haurà de documentar amb detall els procediments de còpia i recuperació de dades que contemplin les accions i els passos necessaris per a l'execució dels processos. Els procediments de recuperació han de garantir la reconstrucció a l'estat en què estaven les dades en el moment de produir-se la pèrdua (o en el moment que s'indiqui per part de l'OTCSL) i han de contemplar la recuperació de les dades tant a nivell de fitxer com de sistema.

Cal destacar que la còpia ha d'assegurar la recuperació no només de les dades sinó també de les configuracions, aplicacions, fitxers de traces (tipus logs), etc.

4.3 Disponibilitat del servei

S'ha de garantir la disponibilitat del servei durant les 24 hores del dia, els 365 dies de l'any. En els casos en què s'hagi de procedir a la realització de tasques de manteniment, actualitzacions o millores en els equips, programari o infraestructures, o de qualsevol altre element implicat en el servei objecte del contracte, haurà de procedir a la seva planificació, intentant reduir en la mesura que es pugui, els talls en el servei.

Els treballs programats s'executaran a la finestra de temps que perjudiqui menys als usuaris i, en tots els casos, haurà de ser autoritzada per l'OTCSL. Les tasques programades s'hauran de notificar a l'OTCSL amb un mínim de 2 dies laborables. Aquest requisit de notificació no serà d'aplicació en aquelles actuacions que tinguin per objectiu resoldre una incidència de caràcter crític, és a dir, quan es produeixi una pèrdua o s'observi el risc d'una pèrdua total del servei.

En relació a la disponibilitat del servei es treballarà a partir dels conceptes següents:

- Disponibilitat del servei. Es defineix com la disponibilitat d'accés per part dels usuaris.
- Període de mesura. S'estableix en hores de servei i es calcula per mesos. Es computaran tots els mesos per 30 dies de 24 hores, per tant, una disponibilitat de 720 hores mensuals.
- Excepcions al nivell de disponibilitat: actuacions d'operacions planificades i incidències de tercers que pugin afectar al servei.

El contractista haurà de vetllar per procurar la màxima disponibilitat del servei. Es penalitzarà la disponibilitat inferior al 99,98%.

L'empresa adjudicatària haurà de presentar mensualment un informe de gestió del servei, incloent el percentatge de disponibilitat del servei d'aquell mes. També haurà d'informar de les incidències detectades (indicant el motiu, la data, hora inici/fi) i les solucions aportades.

4.4 Accés/servei remot

L'allotjament extern ha de donar la possibilitat de connexió als servidors per part de l'empresa contractista, com a responsable del manteniment, i per part del personal de l'OTCSL, com a

responsables de la informació i dels recursos de la IDEBarcelona, així com també per part de tercers que hagin d'executar serveis en aquests servidors (sempre sota el control de l'OTCSL)

Cal assegurar el bon funcionament del servei remot, així com també facilitar la càrrega de grans volums puntuals d'informació.

També cal assegurar els mecanismes adients per a un correcte manteniment i instal·lació del programari, així com de les dades des del CPD, més tenint en compte el volum que pot tenir la informació geogràfica.

4.5 Monitorització del servei

S'ha de preveure el disseny i implantació d'un Pla de Continuïtat del Servei i els mecanismes necessaris per realitzar *fail-over* i *fail-back* de manera automatitzada. El Pla ha de ser automàtic i s'ha d'executar de forma desatesa, o com a mínim sense la participació obligatòria del personal de l'OTCSL.

Es generaran alertes i s'executaran accions immediates per part de l'adjudicatari per solucionar els problemes detectats. És imprescindible que l'OTCSL rebi aquestes alertes per correu electrònic amb caràcter informatiu.

Per assegurar la continuïtat, l'adjudicatari ha de fer una monitorització avançada dels sistemes 24x7 que tinguin en compte, com a mínim:

- **Disponibilitat de les màquines:** Ha d'implementar mecanismes per verificar la disponibilitat de les màquines. Lliurarà un informe mensual a l'OTCSL sobre la disponibilitat diària i continuada dels servidors de producció.
- **Disponibilitat dels serveis:** Ha de garantir l'operativitat i el correcte funcionament dels serveis HTTP/HTTPS, FTP, SMTP i RDP (o equivalent), així com restablir-los immediatament en cas de caiguda.

El servei més crític és HTTP/HTTPS, que suporta les aplicacions web de la plataforma, per tant, també caldrà detectar i resoldre colls d'ampolla per excés de tràfic HTTP/HTTPS.

- **Disponibilitat de la infraestructura:** Ús de CPU, memòria i disc. S'establiran límits de funcionament esperat i es generarà una alerta si es superen.
- **Disponibilitat d'aplicacions:** Ha de monitoritzar les aplicacions que s'estableixin amb l'OTCSL a l'inici del contracte, per verificar que estan disponibles. En cas de fallada, és prioritari detectar-ho i restablir-les immediatament. Durant el període del contracte l'OTCSL pot anar afegint altres aplicacions a la monitorització.
- **Bases de dades:** Ha de garantir que les bases de dades estiguin operatives i funcionin correctament. També cal supervisar la finalització correcta de determinats *jobs*.
- **APIs:** Garantir el rendiment i la disponibilitat de les APIs que ofereix la plataforma.

- **Històric de càrrega i estrès del sistema:** Ha de facilitar indicadors i gràfics amb temps de resposta per identificar punts de fallada, especialment sota alta càrrega.

A més, com a manteniment preventiu, l'adjudicatari ha de planificar reinicis regulars dels servidors en períodes de baixa activitat i també automatitzar l'execució d'scripts de reinici d'aplicacions, sempre previ acord amb l'OTCSL.

L'empresa adjudicatària haurà de documentar la política establerta per a la monitorització de tots els elements aquí descrits, detallant els controls que es porten a terme per assegurar el funcionament de tots els components i el temps de resposta en cas de problemes. També haurà de documentar els *scripts* que prepararà per a possibles reinicis de serveis i aplicacions i el flux d'actuacions quan s'activin les alarmes.

L'OTCSL donarà suport en la definició de què i com monitoritzar, pel que fa als serveis/aplicacions pròpies. I haurà de validar el document presentat per l'adjudicatari on detalli aquesta monitorització.

4.6 Servei d'atenció, suport i manteniment

Els dubtes, consultes, peticions d'actuacions per part dels tècnics de l'OTCSL i els problemes/incidències hauran de ser atesos a través d'un servei d'atenció que assegurï, com a mínim, una disponibilitat en horari laboral (de dilluns a divendres de 08:00 a 20:00). Totes elles han de poder ser ateses via telèfon, e-mail o aplicació de tipus *helpdesk*, sempre assegurant-ne la traçabilitat per tal que des de l'OTCSL es pugui conèixer en qualsevol moment el seu estat de resolució. Les urgències per a problemes crítics en el servei hauran de poder ser sempre tractades i ateses per telèfon, a més d'altres canals, també amb traçabilitat.

Pel que fa a nivell de servei, caldrà assegurar que el temps de notificació d'alertes serà inferior a 1 minut, i que el temps de resposta a les incidències del servei serà inferior a 5 minuts. Aquestes alertes es rebran també per e-mail a les bústies que es designin.

L'empresa serà la responsable de la gestió/administració de la plataforma, assegurant una resposta als problemes de rendiment que es puguin detectar durant el període del contracte. També s'ocuparà del manteniment del maquinari, assegurant una observació setmanal, neteja de fitxers de *log* que no contenen informació útil per al càlcul d'estadístiques d'accés (davant de qualsevol dubte l'adjudicatari demanarà sempre el vistiplau de l'OTCSL per esborrar fitxers), detecció i avís d'incidències. També s'ha de comprometre a intervenir en cas d'incidències o problemes de rendiment, modificar les regles del *firewall* si s'escau, configurar i parametritzar el programari de base, a més d'analitzar i fer *tuning* de les bases de dades incloses al sistema. Es donarà també suport a l'administració de les bases de dades de la plataforma (incloses les bases de dades espacials).

Totes les hores necessàries per a la realització de tasques de suport ordinari sobre els servidors (suport de nivell 1 i 2, monitorització, còpies de seguretat, gestió del projecte, restauració de *backup*,...) estan a càrrec de l'empresa adjudicatària. Addicionalment al suport ordinari que comporta el servei d'allotjament, aquest contracte inclou l'obligació de suport en l'evolució de versions tant del programari de base com de les bases de dades (incloses les espacials), modificació de polítiques de *backup* i en general a projectes nous que impliquin canvis en les configuracions tancades, amb una dedicació mínima de 150 hores/any.

5. Comunicacions

L'empresa adjudicatària proveirà un accés a Internet amb un ample de banda mínim de 50 Mbps en format percentil 95, bidireccional, amb absorció dels pics de càrrega. Aquest ample de banda haurà de poder-se distribuir entre els servidors a mesura que sigui necessari.

La comunicació del CPD amb l'OTCSL i amb tercers la proveirà l'adjudicatari mitjançant connexió segura (VPN) amb un ample de banda d'alta capacitat, assegurant la privacitat i la màxima seguretat, a través de protocols com l'autenticació en dues fases (2FA) o similar.

L'empresa adjudicatària s'encarrega de la provisió i administració dels seus equips de comunicacions, necessaris per garantir la disponibilitat i continuïtat dels serveis objecte d'aquest plec, tant per a les aplicacions web com per a la connexió de l'OTCSL i de tercers al CPD.

La infraestructura de telecomunicacions, arquitectura, mecànica i de seguretat ha de tenir com a referència els indicadors de l'estàndard TIER de l'*Uptime Institute*. Les empreses han d'indicar la qualificació del CPD principal i secundaris segons aquest estàndard. En el cas del CPD principal es requereix mínim TIER III en disseny i construcció.

L'adjudicatari prestarà un servei de Centre d'Operacions de Seguretat (SOC), que inclogui totes les eines necessàries, hardware, software llicències i serveis professionals que siguin necessaris per a la prestació del servei per a tots els servidors, amb un correcte funcionament, sense cap cost addicional al del contracte. Haurà de complir els requisits mínims de seguretat que permetin detectar i prevenir intrusions, bloquejar atacs, etc.

6. Migració de la plataforma entre empreses de *hosting*

En el cas que l'empresa adjudicatària sigui diferent a la contractada actualment, les operacions necessàries per al canvi de servei i prestacions les ha d'assumir l'adjudicatària, i estan incloses al contracte.

Aquesta migració es realitzarà en un termini màxim de 30 dies un cop formalitzat el contracte. Cal tenir en compte que per tal de garantir una correcta continuïtat en la prestació del servei, la migració s'haurà fer prèviament a la finalització del servei de l'empresa sortint.

L'empresa adjudicatària haurà de detallar els procediments i activitats de cada una de les etapes del servei.

6.1 Adquisició de coneixement

Un cop formalitzat el contracte, l'empresa adjudicatària haurà d'adquirir els coneixements necessaris per planificar la transició. Per aquest motiu sol·licitarà tota la informació necessària a l'OTCSL i a l'empresa sortint, amb l'objectiu d'assegurar una transferència entre els *hostings* sense incidències ni pèrdua de servei. El canvi ha de ser pràcticament transparent per als usuaris.

En aquesta fase cal portar a terme les següents funcions:

- Proporcionar un Pla de Migració que cobreixi des de la fase d'adquisició de coneixement fins a la prestació del servei
- Definir un calendari per fer-se càrrec del servei tenint en compte els terminis indicats en el present plec
- Assignar personal capacitat, indicant rols i responsabilitats
- Comunicació contínua amb l'OTCSL

6.2 Migració dels serveis

Un cop aprovat el Pla de Migració per part de l'OTCSL, es començarà amb la migració dels serveis.

Atenent que l'actual servei d'allotjament està implementat en servidors virtuals VMware, es suggereix la utilització de les eines d'exportació/importació per a la migració dels servidors (tenint en compte aquesta tecnologia i la versió que s'utilitza en els servidors actuals).

En aquesta fase es realitzaran les activitats necessàries que permetin la continuïtat del servei i també l'evolució del model d'explotació del servei, conforme als requeriments establerts a la proposta de l'empresa adjudicatària.

En aquesta fase conviuran simultàniament l'anterior adjudicatari i el nou, el qual haurà de realitzar les activitats necessàries per a la transformació del servei, sense que suposi un perjudici a les tasques de l'adjudicatari sortint ni a la qualitat dels serveis que presta l'OTCSL a través d'aquesta plataforma.

De cara al seguiment i control de qualitat inicials, caldrà establir un calendari de reunions per assegurar una correcta posta en marxa i assegurar-ne la viabilitat.

6.3 Prestació del servei

Un cop finalitzada la instal·lació, el proveïdor del servei certificarà el funcionament de tots els elements de la plataforma i començarà la presa de control, fent-se responsable del suport, manteniment i operació de la plataforma. A més, proporcionarà a l'OTCSL la documentació de la solució implantada.

Aquesta etapa es considera l'inici de la prestació del servei sota el model que consta al document d'oferta de la licitació, moment en que l'adjudicatari estarà obligat a complir amb el nivell de servei establert.

6.4 Devolució del servei

En el cas de canvi de proveïdor, l'adjudicatari es compromet a cooperar i a facilitar la transferència dels serveis al futur adjudicatari. Durant el període de devolució, l'adjudicatari realitzarà una proposta de pla d'execució a seguir per tal de garantir la continuïtat del servei, donant una importància especial a la gestió de riscos associats, amb l'objectiu de minimitzar l'impacte en el servei.

El Pla de devolució del servei s'ha de lliurar en el termini màxim de 15 dies des de la notificació oficial d'extinció total o parcial del servei.

Els aspectes mínims que cal assegurar en aquesta fase són:

- Una metodologia i documentació per transferir el coneixement dels punts fonamentals de les operacions i projectes en curs de l'OTCSL.
- Un Pla de reversió que inclogui la planificació d'activitats, els responsables i la gestió de la resolució de les incidències entre el nou proveïdor, l'OTCSL i altres possibles proveïdors.
- Un Pla de lliurement de totes les còpies de que disposi amb informació de l'OTCSL, i la destrucció, de forma fefaent, de les que no siguin portables, aportant un certificat de lliurament i destrucció.
- Garantir la prestació del servei, essent d'aplicació tots els requisits establerts en aquest Plec.
- Garantir l'estricta compliment de les mesures de seguretat previstes per l'Esquema Nacional de Seguretat (ENS) per a la informació en trànsit durant el procés de migració al nou adjudicatari.

La prestació del servei no finalitzarà fins que la Devolució del servei estigui finalitzada a criteri de l'OTCSL, als efectes de garantir que el nou proveïdor disposa del control total del servei.

Les empreses contractants han d'incloure a l'oferta tècnica una proposta de Pla de devolució del servei pel cas en que sigui necessari a la finalització aquest contracte.

7. Equip de treball tècnic

Les empreses han de proposar l'equip de treball tècnic que portarà a terme els treballs. Els tècnics designats pel contractista seran de qualificació i experiència apropiada a les comeses que han de realitzar. L'equip estarà integrat com a mínim per dos enginyers informàtics, o titulació equivalent, un dels quals ha de ser expert en l'administració de base de dades Oracle (DBA), amb una experiència mínima de dos anys en aquest tipus de base de dades i ha de tenir coneixements d'administració de bases de dades PostgreSQL per si eventualment es requereix treballar amb aquest gestor de base de dades. El responsable tècnic del servei, interlocutor tècnic amb l'OTCSL, haurà de ser un enginyer informàtic.

En el cas que algun tècnic no reuneixi les condicions abans assenyalades, segons l'opinió del responsable de la Diputació de Barcelona, serà notificada aquesta circumstància a l'empresa contractista a fi que procedeixi a la seva substitució en l'execució de les esmentades tasques.

Si durant l'execució del contracte l'empresa adjudicatària ha de canviar alguna persona designada, ho podrà fer sempre prèvia informació a l'OTCSL, sense que suposi una reducció en la qualitat dels treballs ni dels coneixements.

8. Seguretat i qualitat

8.1 Seguretat i qualitat del servei

El CPD ha d'incloure la provisió i administració de mesures de seguretat i qualitat de servei:

- Serveis de seguretat perimetral: Routers segurs, firewalls, sistemes de rebuig d'intrusions, antivirus, antispam i tot el que sigui necessari, amb l'objectiu de protegir al màxim els servidors, accessos i aplicacions front a possibles atacs.
- Implementació de mesures necessàries per evitar els atacs de denegació de servei (DoS), de denegació de servei distribuït (DDoS) i altres tipus de ciberatacs.
- Gestió d'actualitzacions crítiques de seguretat: Instal·lació i seguiment de les instal·lacions i pedaços crítics de programari dels servidors per tal de mantenir la seguretat constant, així com la seva configuració segura, prèvia comunicació i acord amb l'OTCSL.
- Disponibilitat d'un segon CPD per a casos de recuperació front a un desastre del CPD principal, de manera que es garanteixi la disponibilitat dels serveis en un període màxim d'una hora.
- Seguretat física que ha de contemplar com a mínim: Alimentació elèctrica ininterrompuda (amb SAIs), sistema de detecció i extinció d'incendis, climatització òptima controlada amb sistemes d'aire condicionat redundat, sistemes de seguretat física amb càmeres de seguretat i vigilància 24x7.
- Disponibilitat d'un sistema de traces (logs o similar) amb una estratègia de retenció suficient que permeti fer una anàlisi davant d'un incident i que permeti gestionar el nivell adequat de traces segons es requereixi.

Durant tot el temps que duri el servei d'allotjament, l'OTCSL podrà establir controls de qualitat del servei, segons estimi oportú, mitjançant reunions presencials a les seves oficines, si s'escau.

8.2 Seguretat de la informació

L'empresa contractista estarà obligada a implementar les mesures de seguretat necessàries per donar compliment als requisits que s'estableixen a la Llei orgànica 3/2018, de 5 de desembre, de Protecció de dades Personals i garantia dels drets digitals, a la seva Disposició addicional primera, sobre Mesures de seguretat a l'àmbit del sector públic. Així cal seguir el que al respecte es diu al "Reial Decret 3/2010, de 8 de gener, pel que es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'administració Electrònica", en la categoria que determini la Diputació i el que estableix el "Reglament europeu 2016/679, 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 (RGPD)". Sobre aquest assumpte cal tenir en compte també el que es diu al Plec de clàusules administratives particulars (PCAP) i el que es pugui establir a les normatives sectorials al respecte.

De la mateixa manera l'empresa contractista vetllarà per l'acompliment de les obligacions de confidencialitat i deure de secret del seu personal pel que fa a les dades de caràcter personal (veure el PCAP), als sistemes d'informació i a qualsevol altre informació o recurs corporatiu que hi puguin tenir accés en el decurs del present contracte.

Si s'escau, tots els dispositius que intervinguin en l'execució d'aquest contracte hauran d'estar configurats per a l'eliminació d'arxius de dades temporals, permetent eliminar els residus del material confidencial que s'originen a l'hora de digitalitzar, imprimir, copiar i enviar correu electrònic o via aplicacions de tipus *helpdesk* diàriament.

En qualsevol cas, el contractista no podrà accedir als documents, arxius, sistemes i suports que continguin dades de caràcter personal sense autorització expressa de l'òrgan competent de la Diputació. En el cas que el personal vinculat a l'empresa contractista tingués accés, directe o indirecte, a dades o informacions de caràcter personal, l'empresa els exigirà el compliment del deure de secret respecte de les dades i informacions a què haguessin pogut tenir accés en el desenvolupament de l'activitat o servei prestat.

En el cas que el contractista destini les dades a les quals tingui accés a una finalitat diferent a l'establerta, o les comuniqui o les utilitzi incomplint les estipulacions del contracte o les instruccions de l'Administració Contractant, el contractista serà considerat responsable del tractament i respondrà personalment de les infraccions que hagi comès i de les possibles reclamacions que es puguin produir al respecte.

L'empresa contractista ha d'indicar el nivell vigent de compliment de l'ENS (Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat), que ha de ser, com a mínim, mitjà. El nivell de seguretat s'ha d'aplicar a tot el servei: allotjament, assistència tècnica i suport. Cal mantenir el nivell de l'ENS durant la vigència d'aquest contracte. També ha de disposar del certificat vigent de seguretat d'acord amb l'estàndard internacional ISO 27001 (Sistemes de gestió de la seguretat de la informació), assegurant-ne la vigència durant tot el contracte. Amb aquestes dues certificacions es pretén assegurar una bona gestió de la ciberseguretat.

9. Responsabilitat del servei

La responsabilitat del servei estarà a càrrec de l'empresa contractista, qui haurà de designar un responsable del servei a nivell directiu, que actuarà com a interlocutor en els casos en que hi hagi problemes que no es puguin resoldre a nivell tècnic i que garanteixi el compliment de les obligacions contractuals.

L'empresa no utilitzarà les dades ni la informació allotjada per part de la Diputació de Barcelona. Només utilitzarà el necessari per prestar els serveis contractats d'allotjament web i comunicacions. En cap cas l'empresa utilitzarà o aplicarà les dades contingudes als servidors, així com la resta d'informació allotjada per la Diputació de Barcelona a finalitats diferents de les establertes al present contracte.

Un cop finalitzat el servei, i traspassat tot l'entorn a una nova plataforma, l'empresa contractista s'obliga a destruir la totalitat d'informació i components a que hagués tingut accés durant la prestació del servei.

10. Contingut i estructura de les ofertes tècniques

Els licitadors presentaran una proposta tècnica amb la descripció i especificacions de tots els components i serveis de l'oferta, de manera que es pugui comprovar que compleixen els requisits descrits en aquest plec.

Totes les ofertes hauran de tenir un índex on es referenciïn els diferents apartats del Plec de Prescripcions Tècniques als efectes de facilitar-ne la valoració. En referència al contingut, hauran de donar resposta als requeriments del plec i ajustar-se al següent format:

10.1 Presentació

Presentació de l'empresa licitadora, indicant els àmbits en els que treballa, els seus objectius i projectes similars als d'aquest procediment obert.

10.2 Resum de la solució tècnica

Resum de la solució proposada descrivint, com a mínim, la infraestructura dels serveis, les característiques operatives, el sistema de gestió, les utilitats d'operació i manteniment, els paràmetres de qualitat, la disponibilitat, les eines utilitzades i l'arquitectura del sistema.

Es detallarà també:

- Nivell vigent de classificació TIER dels CPD primari i secundari
- Nivell vigent de certificació ENS (RD 311/2022) de l'empresa
- Disponibilitat vigent de les certificacions ISO 9001, 20000, 27001, 27017, 27018, 22301 (si s'escau)
- Ubicació física dels CPD primari i secundari
- Nom i titulació dels tècnics designats, de l'interlocutor tècnic i del responsable del servei (interlocutor directiu)

10.3 Pla de continuïtat del servei

Es proposarà un Pla de continuïtat del servei on es detalli el pla de còpies de seguretat, les actuacions en el cas de caiguda del CPD primari i el conseqüent procés de *rollback* un cop recuperat.

10.4 Pla de migració

Es descriuran les tasques de la fase de migració inicial de servidors fins a l'assumpció del servei. Cal aportar un calendari aproximat de fites.

10.5 Pla de devolució

Es farà una proposta de Pla de devolució del servei on es detallaran els passos a fer, en el cas que es requereixi en finalitzar aquest contracte.

Metadades del document

Núm. expedient	2024/0029002
Tipus documental	Plec de clàusules o condicions
Títol	Allotjament SITMUN 2024 - PlecTècniques
Codi classificació	D0506SE01 - Serveis obert

Signatures

Signatari		Acte	Data acte
Joan Closa Pujabet (SIG)	Responsable directiu Servei Promotor	Signa	25/10/2024 12:08

Validació Electrònica del document

Codi (CSV)	Adreça de validació	QR
ce90349c4dab40f531a6	https://seuelectronica.diba.cat	

