Àrea de Serveis Generals i Transició Digital
Direcció de Serveis de Tecnologies i Sistemes Corporatius

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA CONTRACTACIÓ D'UNA SOLUCIÓ INTEGRAL (SaaS)DE GESTIÓ DE LA CÒPIA DE SEGURETAT I RESTAURACIÓ, AL NÚVOL, DE LA PLATAFORMA MICROSOFT 365 DE LA DIPUTACIÓ DE BARCELONA

Exp. 2026/0004487

Índex

1. Antecedents

La Direcció de Serveis de Tecnologies i Sistemes Corporatius (DSTSC) de la Diputació de Barcelona té com a missió proporcionar tots els serveis i infraestructures d'informàtica i telecomunicacions de la Diputació de Barcelona, per a l'àmbit intern i també donar suport als ens locals, establint estratègies de futur alineades amb les necessitats funcionals corporatives i optimitzant la relació cost-benefici.

Els serveis de tecnologies i sistemes corporatius s'entenen com la integració dels àmbits clàssics de la informàtica i les telecomunicacions. S'assegura una direcció única per al tractament lògic de la informació i les seves xarxes de transmissió, independentment del seu format físic (veu, dades o imatge).

Les funcions assignades a la DSTSC són:

- Dur a terme els criteris fixats per la Diputació de Barcelona en matèria de tecnologies de la informació (en endavant TIC). És a dir, informàtica, telecomunicacions i, en general, aquelles tecnologies relacionades amb el tractament automatitzat de la informació, i proposar els recursos necessaris que cal habilitar per a aquesta finalitat.
- Coordinar les tasques administratives de TIC de totes les unitats de la Diputació de Barcelona i, de forma particular, aquelles que tenen interrelació, i proposar les mesures adequades per a una màxima normalització.
- Controlar i fer el seguiment d'aquelles tasques en matèria TIC realitzades per a la Diputació de Barcelona mitjançant recursos externs.
- Proposar i gestionar les actuacions a desenvolupar per la Diputació de Barcelona en matèria TIC que, dins dels supòsits de la cooperació i assistència, es realitzin per als ens locals de la província de Barcelona.
- Desenvolupar i gestionar els projectes en TIC que es produeixin a proposta de les àrees, direccions i serveis de la Diputació de Barcelona.
- Coordinar la formació i reciclatge del personal de la Diputació de Barcelona en matèria TIC.
- Informar de la despesa econòmica que generin les àrees, direccions i serveis de la Diputació de Barcelona i els seus organismes autònoms en matèria TIC.
- Assessorar els organismes autònoms de la Diputació de Barcelona en matèria TIC, quan així es requereixi i tutelar, si escau, l'homogeneïtat en el tractament dels sistemes d'informació comuns.
  Prestar suport per a l'adequació corporativa a l'acompliment de la normativa de protecció de dades i de l'Esquema Nacional de Seguretat, en els aspectes jurídics, organitzatius i tecnològics dels tractaments que duu a terme la Diputació de Barcelona, no només com a responsable d'aquest tractament per als ens locals sinó també com a encarregada.

Pel que fa a l'objecte específic d'aquest expedient, la DSTSC utilitza Microsoft 365 per als empleats de la Diputació de Barcelona, d'alguns ajuntaments i dels treballadors de la Xarxa de Biblioteques de la Diputació.

Totes les dades que els usuaris emmagatzemen en qualsevol de les utilitats de l'entorn Microsoft 365 (Outlook -Exchange online-, Share Point, Microsoft Teams, OneDrive i Groups) s'emmagatzemen als repositoris de Microsoft al núvol.

Per tal de garantir completament la disponibilitat davant de qualsevol atac, aturada o incident de les dades al núvol, així com per a adaptar el servei a les polítiques de còpia i restauració aprovades per la Diputació de Barcelona, la DSTSC considera necessari disposar d'una còpia de les dades fora de l'entorn Microsoft 365 i fora de l'entorn corporatiu.

En concret:

- Adaptar els temps de retenció de les còpies de seguretat, als criteris que consideri més adients la DSTSC.
- Adaptar els criteris de granularitat de la restauració de les dades, a les necessitats de la DSTSC.

2. Objecte

És objecte del present plec definir les especificacions tècniques particulars per a la contractació d'una solució integral de gestió de la còpia de seguretat i restauració, al núvol, de la plataforma Microsoft 365 de la Diputació de Barcelona.

3. Abast

L'empresa contractista haurà de proporcionar una solució integral, amb tots els elements necessaris per a la prestació del servei (entès com una solució completa i integrada) que inclogui la capacitat de copiar i restaurar, segons les especificacions i requeriments establerts en el present Plec, de totes les dades generades a la plataforma Microsoft 365 de la Diputació de Barcelona, pel que fa als usuaris llicenciats, així com, tot el servei d'infraestructura i sistemes de base (en sentit ampli) necessaris per a la correcta prestació del servei. Les dades a copiar i restaurar seran, com a mínim, les de les següents aplicacions incloses dins de la plataforma Microsoft 365:

- Outlook (Exchange Online).
- Share Point.
- Microsoft Teams.
- OneDrive.
- Groups.
- EntraID.

L'empresa contractista haurà de dimensionar la infraestructura i els sistemes de base necessaris per a la prestació del servei, per proporcionar la capacitat de processament i l'espai d'emmagatzematge suficient per desar totes les còpies generades amb la retenció definida per la DSTSC, durant la totalitat de la vigència del contracte. La capacitat d'emmagatzematge de la solució haurà de ser la suficient per poder allotjar les còpies de seguretat amb la retenció definida per la DSTSC.

En cas que s'hagi d'incrementar d'aquest dimensionament, no representarà cap cost addicional per a la Diputació de Barcelona.

En cap cas, el cost del contracte es veurà afectat pel volum de dades transmeses al servei de còpies i restauració.

L'empresa contractista també aportarà, tot el programari i les eines de seguretat necessàries, per a garantir la privacitat de les dades.

4. Descripció del contracte

El contractista haurà de proveir una solució completa i integrada de còpia de seguretat i de restauració, per mantenir les còpies de totes les dades generades per l'ús de les aplicacions de Microsoft 365 al núvol de Microsoft, per a tots els usuaris que disposen de llicències a la Diputació de Barcelona.

La Diputació de Barcelona podrà decidir cada quant temps es realitza la còpia de les dades i durant quant temps es manté la retenció de cadascuna de les còpies. Els tècnics de la DSTSC seran els únics que accedeixin a les còpies per restaurar les dades necessàries i realitzaran les tasques d'administració de la solució.

El servei contractat estarà format per dues fases: la primera fase, amb una vigència de 3 anys, correspon a la realització de còpies de seguretat i restauracions amb la modalitat de llicència backup (còpia) i restore (restauració) M365 (cl. 4 i 5 d'aquest Plec); i una segona fase, amb una vigència d'un any i que només s'activarà en cas que hi hagi alternança entre contractistes, a la qual es realitzaran únicament restauracions, amb l'objectiu de poder restaurar en qualsevol moment, si es necessita, les còpies no expirades (cl. 9 d'aquest Plec). La modalitat de llicència aplicable a la segona fase serà exclusivament la de *Llicència Restore M365*.

L'empresa licitadora proposada com a adjudicatària, en els terminis que preveu la clàusula 1.18 del Plec de clàusules administratives particulars, haurà d'acreditar, abans de l'adjudicació, que compleix amb els següents requisits:

Certificació Élite, Gold o equivalent de l'empresa fabricant del software proposat.

4.1. Requeriments funcionals

En aquest apartat es descriuen els requeriments funcionals que ha de complir la solució, en concret:

- **Accés al programari de gestió a través d'un navegador web**
  Per accedir a qualsevol funcionalitat de gestió es farà a través d'un navegador web. No serà necessària, la instal·lació de cap programari en l'equip de la persona que hi accedeixi.

- **Autenticació d'usuaris**
  La solució no emmagatzemarà cap usuari, ni contrasenya. La validació dels usuaris es farà mitjançant l'estàndard SAML amb l'eina de gestió d'identitats de la DSTSC. Únicament existirà un usuari local en el sistema, que s'utilitzarà en el cas que el sistema de gestió d'identitats de la DSTSC estigui fora de servei.

  El sistema ha de permetre limitar les adreces IP des d'on es connecten els usuaris a la solució i bloquejar l'accés des de la resta d'adreces IP no autoritzades per la DSTSC.

- **Log de moviments**
  El sistema disposarà d'un log on quedaran registrats, com a mínim, els següents esdeveniments:

  - Data, hora i usuari dels accessos vàlids.
  - Data, hora i usuari dels intents d'accés no vàlids.
  - Data, hora i usuari de les creacions, modificacions o eliminacions de polítiques de còpies de seguretat.
  - Data, hora, usuari i descripció de les dades recuperades de la còpia de seguretat.

- **Control d'accés basat en rols**
  La solució ha de permetre l'assignació de diferents rols als usuaris autoritzats per poder interactuar-hi, sempre sota la premissa del principi del mínim privilegi. Com a mínim, haurà de permetre assignar els rols següents:

  - Configurar còpies de seguretat.
  - Recuperar còpies de seguretat (sense poder veure el contingut dels correus i fitxers de les còpies de seguretat).
  - Recuperar còpies de seguretat (podent veure el contingut dels correus i fitxers de les còpies de seguretat).

- Visualitzar el log de registre.
- Recuperar còpies de seguretat d'usuaris marcats amb la funcionalitat "Dret de ser oblidats".
- Afegir/eliminar/modificar usuaris i rols.

- **Productes de Microsoft 365 coberts per la solució**
  La solució de còpia de seguretat ha de poder protegir i recuperar (a la mateixa ubicació i a una ubicació alternativa), com a mínim, els següents elements de Microsoft 365:

  - Microsoft Exchange:
    - Bústies de correu electrònic dels usuaris.
    - Bústies departamentals o grupals.
    - Carpetes Públiques.
    - Calendaris.
    - Contactes.

  - SharePoint:
    - Fitxers.
    - Versions dels fitxers.
    - Directoris.
    - Biblioteques.
    - Llistes i elements de llistes.
    - Llocs Teams i subllocs.
    - Notebooks.
    - Pàgines.
    - Permisos.
    - Formularis.
    - Plantilles.

  - OneDrive:
    - Fitxers.
    - Versions dels fitxers.
    - Directoris.

  - Teams:
    - Teams d'equips públics, privats i de tota l'organització.
    - Channels de canals regulars i privats.

- Tabs de publicacions, fitxers, wiki, llocs web, Word, Excel, PowerPoint i PDF, biblioteques de documents, noms, tipus i ajustament de pestanyes.
- Converses i post (elements de les converses i les respostes).
- Calendaris.
- Fitxers.

- Grups:
  - Grups creats en Yammer, Planner i Outlook.

- Identitats i objectes Microsoft Entra ID:
  - La solució haurà de ser capaç d'efectuar còpies de seguretat d'objectes d'identitats i accessos disponibles a Microsoft Entra ID, incloent, com a mínim:
    - Usuaris.
    - Grups.
    - Rols.
    - Logs d'activitat.
    - Unitats administratives.
    - Claus de xifrat Bitlocker.

La restauració d'aquests objectes haurà de poder efectuar-se sobre el mateix núvol de Microsoft y a una ubicació alternativa.

- **Autodescobriment d'usuaris Microsoft 365**
  La solució haurà d'autodescobrir els usuaris nous de la plataforma Microsoft 365 de la Diputació de Barcelona, no requerint cap intervenció manual per part dels tècnics per afegir un nou usuari (de qualsevol de les aplicacions incloses a l'apartat Abast del present Plec). La solució l'afegirà a la còpia de seguretat de manera automàtica. Aquesta funcionalitat haurà de permetre configurar els usuaris a copiar a través de grups d'Active Directory.

- **Configuració de la planificació i la retenció**
  La solució ha de permetre efectuar, de manera automàtica i desatesa, com a mínim, una còpia de seguretat al dia. També, haurà de permetre efectuar còpies "on demand".

  El sistema haurà de permetre configurar la retenció de cada còpia, limitant el període de retenció de cadascuna d'elles. La retenció mínima serà d'un any i haurà de poder ser ampliable fins a 3 anys, sense que això suposi cap cost addicional per a la Diputació de Barcelona.

- **Cercador de documents**
  Disposarà d'un cercador que permeti localitzar documents, dintre dels backups, a fi de facilitar les tasques de cerca i filtrat per a localitzar la informació, canals de converses, fitxers, Teams o correus electrònics a restaurar. El cercador haurà de permetre la indexació per a localitzar les dades de manera àgil, independentment del nombre de còpies retingudes.

- **Dret a l'oblit**
  Amb l'objectiu de complir amb el GDRP, la solució ha de disposar de la capacitat de marcar còpies de seguretat amb una funcionalitat que permeti identificar i bloquejar informació, per tal d'evitar que es pugui restaurar de manera estàndard, també coneguda com a *dret a l'oblid* o *right to be forgotten*.

  Quan una informació de còpies de seguretat d'un usuari s'identifiqui amb aquesta característica, aquestes dades només podran ser restaurades per un usuari amb drets elevats diferent dels usuaris que restauren de manera ordinària.

Tipus de restauracions permeses per la solució

La solució de còpia de seguretat ha de permetre restaurar, com a mínim, els elements següents amb la granularitat següent:

- Microsoft Exchange:
  - Restaurar una bústia completa, incloent correus, calendaris i contactes.
  - Restaurar correus, calendaris i contactes de manera granular a un fitxer PST o fitxers independents (.eml, ics, vcf...), a la bústia origen i a una bústia diferent.
  - Restaurar dades de bústies eliminades.
  - Objectes eliminats.

- SharePoint:
  - Sites.
  - Fitxers, incloent fitxers de mida superior a 2 GB.
  - Llocs de nivell superior (Top-level site) i sub-sites.
  - Documents, elements de llista i biblioteques eliminades.
  - La restauració s'ha de poder efectuar al lloc original o a altres sites.

- OneDrive:
  - Fitxers.
  - Versions dels fitxers.
  - Directoris.
  - Comptes OneDrive

- Teams:
  - Restauració dels elements especificats en l'apartat anterior que descriu els elements coberts per la solució de Teams.

- EntraID:
  - Restauració dels elements especificats en l'apartat anterior que descriu els elements coberts per la solució d'EntraID.

L'eina haurà de disposar d'una funcionalitat per crear d'una adreça URL única que permeti, un cop validat un usuari amb una contrasenya, accedir a l'eina de backup, només a les dades configurades per a recuperar, perquè el propi usuari pugui efectuar la restauració de les dades. L'eina haurà de permetre configurar una data d'expiració d'aquesta URL.

El nombre de restauracions a realitzar serà il·limitat, sense que això suposi cap cost addicional per a la Diputació de Barcelona.

Suport multi-tenant

L'entorn Microsoft 365 de la Diputació de Barcelona està format per multitud de tenants. Això, vol dir que la solució ha de poder suportar el funcionament multi-tenant, garantint que la capacitat de l'emmagatzematge és la suficient per efectuar els backups de totes les dades, fitxers i bústies creades en els diferents tenants i les retencions que la DSTSC estableixi a les còpies de seguretat, sempre respectant el nombre màxim d'usuaris especificat en el present plec. La DSTSC podrà crear més tenants per adequar-ho al seu creixement i la solució cobrirà els nous tenants.

Les dades dels diferents tenants hauran d'estar aïllades entre elles. El sistema haurà de permetre limitar als diferents usuaris la possibilitat o no de restaurar dels diferents tenants, configurant els rols d'accés per a cada tenant independentment.

4.2. Requeriments tècnics

En aquest apartat es descriuen tots els requeriments tècnics que ha de complir la solució, en concret:

- **Alta disponibilitat**

  La solució ha de disposar dels elements necessaris per a garantir la disponibilitat 24x7. Per a tal efecte, és un requisit indispensable que tots els elements necessaris per al funcionament del servei (servidors, programari, emmagatzematge, comunicacions i elements de seguretat) siguin redundants. Les dades de les còpies de seguretat hauran d'estar simultàniament en dos centres de procés de dades diferents i georedundants. Aquests centres de dades hauran de ser diferents i independents dels centres de dades de Microsoft.

- **Rendiment**

  La solució ha de garantir que està dimensionada en tot moment per poder efectuar les còpies de seguretat i les restauracions amb un rendiment que garanteixi que l'execució de qualsevol còpia no superi una durada de 24 hores (per assegurar que sempre existeixi una còpia diària de totes les dades) i que la restauració d'una bústia de 10 GB no superi els 15 minuts de durada i la restauració d'1 GB de fitxers no superi els 5 minuts. El creixement de les dades de còpies de seguretat emmagatzemades no podrà suposar en cap cas una baixada del rendiment abans indicat.

  El procés de còpia de dades no pot afectar al rendiment de l'ús de la plataforma Microsoft 365.

- **Seguretat**

  La solució haurà de disposar d'un sistema que detecti possibles casos de Ransomware o altres tipus de ciberatacs. Aquesta detecció l'efectuarà analitzant canvis anòmals en les còpies de seguretat que realitzi (modificacions, esborrats, creixements anormals, etc.), els quals podran ser indicatius d'un possible atac de Ransomware, altres tipus de ciberatacs o en situació de corrupció de les dades. Quan la solució detecti aquesta situació, generarà una alerta perquè l'equip tècnic de la DSTSC ho analitzi.

  Totes les dades i metadades emmagatzemades en la còpia hauran d'estar xifrades. L'accés a la plataforma de gestió i internament, a l'emmagatzematge, s'efectuarà en tot moment mitjançant connexió HTTPS.

  S'ha de garantir que les dades de les còpies de seguretat seran immutables, de manera que un atacant no pugui alterar o eliminar aquestes còpies.

La solució ha de comptar amb mecanismes que garanteixin que l'empresa contractista no pugui accedir a les dades de les còpies de seguretat ni a l'entorn Microsoft 365 de la Diputació de Barcelona.

L'empresa contractista ha de disposar d'un pla de resposta a incidents (IRP - Incident Response Planning-) i de procediments de recuperació de desastres (DRP -Disaster Recovery Plans-) que haurà de ser validats i revisats anualment amb els tècnics de la DSTSC.

- **Compatibilitat amb altres sistemes de còpies**

  L'ús del sistema de còpies ha de permetre utilitzar simultàniament, altres sistemes de còpies sobre les dades dels mateixos usuaris.

4.2.1. Usuaris llicenciats (volumetria estimada)

Abans de l'inici de cada anualitat es fixarà el nombre de llicències a utilitzar durant l'any següent. Amb aquesta finalitat, els tècnics de la DSTSC proporcionaran a la contractista, un mes abans de l'inici de l'anualitat, la quantitat de cada tipus de llicència i les dades necessàries per a l'activació.

El nombre de llicències podrà augmentar o disminuir segons les necessitats de la Diputació de Barcelona.

La taula següent detalla una estimació sobre el nombre de llicències actives, a l'inici de cada anualitat prevista, de vigència del contracte.

Fase de còpies i restauracions	Primer any	28.810 llicències
	Segon any	30.110 llicències
	Tercer any	31.410 llicències
Fase de transició del servei	Quart any	Restauració de 31.410 llicències

La taula següent detalla l'estimació de llicències que es podran afegir durant cadascuna de les anualitats del contracte.

Primer any	1.300 llicències
Segon any	1.300 llicències
Tercer any	1.300 llicències

4.2.2. Gestió del monitoratge

El sistema disposarà d'un sistema de monitoratge que informarà, mitjançant correu electrònic configurable pels tècnics de la DSTSC, dels esdeveniments principals esdevinguts, com ara les còpies efectuades, les còpies fallides i incidents de funcionament de la solució de backup.

L'empresa contractista haurà de monitorar la disponibilitat de tot l'entorn administrat de manera ininterrompuda en modalitat 24x7. Això implica:

- Monitorar la disponibilitat de la plataforma de backup.
- Monitorar la connexió entre la plataforma de backup i la infraestructura Microsoft 365.
- Monitorar la utilització de la plataforma detectant usos no desitjats o ciberatacs.
- Monitorar la capacitat del sistema i el seu rendiment.

A partir de l'activitat de monitoratge dels sistemes, l'empresa contractista aplicarà alguna de les accions següents:

- Notificarà els esdeveniments quan siguin detectats i actuarà immediatament (obrint incidència o tasca) davant de talls de servei o ciberatacs.
- Obrirà tasques d'administració per a actuacions de millora de la capacitat.
- Obrirà tasques d'administració per a actualització de components del sistema.

El monitoratge ha de permetre fer una correcta gestió de la capacitat i per tant, ha de servir per proposar actuacions de forma proactiva per evitar que es produeixin caigudes de rendiment o talls de disponibilitat. En el cas que es produeixi alguna incidència, servirà per a poder actuar de forma immediata.

4.2.3. Disponibilitat

Es demana una disponibilitat del 99,7%.

En el casos en què s'hagi de procedir a la realització de tasques periòdiques de manteniment, actualitzacions o millores en els equips, programari o infraestructures, o de qualsevol altre element inclòs en el model SAAS, s'haurà de procedir a la seva planificació, intentant pal·liar, en la mesura del possible, talls en el servei que afectin als usuaris finals de la solució.

Els treballs programats s'executaran en la finestra de temps que menys perjudici ocasioni als usuaris finals de la solució i, en tots els casos, haurà de ser autoritzada per la DSTSC.

Definició de temps de disponibilitat: és la suma del temps, en minuts, en que la solució ha estat disponible durant el període de temps establert com a mesura (un mes natural). Per aquest contracte s'entén com a servei la disponibilitat d'accés per part dels usuaris a les interfícies de consulta pública i d'administració i la seva operativa.

Definició de rati de disponibilitat: és la relació del temps de disponibilitat respecte del temps total en minuts d'un (1) mes natural.

Definició de rati de disponibilitat mínima objectiu: és el rati de disponibilitat mínima que es desitja assolir i s'indica en quantitat de nous (9) del rati, per exemple tres nous seria el 99,9% o quatre nous seria el 99,99%.

Definició de temps de no disponibilitat: és la suma del temps en minuts en que la solució no ha estat disponible durant el mes natural.

Definició de temps de no disponibilitat màxim objectiu: és el temps màxim de no disponibilitat que es desitja assolir i es calcula, com la diferència de minuts, entre el temps total en minuts d'un mes natural computant els dies de 24h.

5. Model de prestació

5.1. Software as a Service

La prestació objecte d'aquesta contractació s'haurà de fer d'acord amb el model de prestació conegut com a Software as a Service (SaaS).

SaaS és una modalitat de solució on el programari i les dades relacionades s'hostatgen en servidors i sistemes d'emmagatzematge a càrrec del proveïdor de la solució i l'accés als mateixos es realitza a través d'Internet de forma segura. Per tant, la informació, el seu processament i els resultats del tractament d'una determinada lògica de negoci estant hostatjats a les instal·lacions del contractista.

El contractista es fa càrrec de tota la infraestructura, maquinari i programari, necessari per a la prestació del servei. És a dir, de qualsevol despesa derivada de la prestació de la solució: del programari, tant a nivell servidor com a client (desenvolupat o llicenciat); del maquinari (físic o virtual, així com qualsevol tipus de llicència associada); i de les comunicacions adients fins a la posada a disposició de la informació a través d'Internet. Així mateix, es farà càrrec de qualsevol actuació que calgui, sigui correctiva, preventiva o evolutiva, per tal de mantenir la solució amb els paràmetres de qualitat i seguretat adients.

Altres requisits que ha de tenir en compte el contractista en relació a aquesta modalitat són:

- La infraestructura per oferir la solució ha d'estar allotjada en territori de la UE.
- No es permet cap tractament de dades personals fora de la UE, ni tan sols per al seu emmagatzematge, ni per a la realització de còpies de seguretat.

- Per a tots els usuaris, totes les comunicacions han d'estar xifrades i han de comptar amb mesures de seguretat adients per a mantenir la confidencialitat, disponibilitat, traçabilitat i integritat de les dades.

- Forma part de la solució la devolució dels logs de moviments i la destrucció de totes les dades, tant les operatives com les còpies de seguretat existents, una vegada finalitzat el contracte. Totes les accions corresponents hauran d'estar certificades.

- El sistema ha de disposar d'alta disponibilitat, tant pel que fa a la pròpia infraestructura, l'equipament de xarxa, línies de dades, elements de seguretat, com al subministrament elèctric i refrigeració d'aire de la infraestructura.

- El contractista estarà obligada a realitzar, al menys, una revisió completa del maquinari a l'any, amb la finalitat d'assegurar el perfecte funcionament del sistema i evitar incidències futures. Aquestes accions hauran d'estar certificades.

En cap cas, la Diputació de Barcelona es farà càrrec dels costos de l'emmagatzematge necessari per a garantir una retenció de les còpies ni del tràfic de xarxa (ni de còpies ni de baixada en les restauracions) durant tota la vigència del contracte, aquestes despeses aniran a càrrec de l'empresa contractista.

5.2. Formació

El contractista garantirà la formació actualitzada en l'ús del sistema de còpies durant tota la durada del contracte.

El contractista dedicarà un mínim de dues hores mensuals a temes de formació contínua en l'ús de l'eina, sempre sota demanda dels tècnics de la DSTSC. Aquest temps també servirà, si escau, per resoldre dubtes tècnics i funcionals que sorgeixin arran de l'ús del sistema.

5.3. Gestió de les incidències

Es tracta d'aquelles actuacions que tenen com a objectiu resoldre disfuncions en el funcionament de la solució contractada i que tendeixen a minimitzar el nombre d'incidències i la seva resolució, en el mínim temps possible, fins i tot, si es deriven de la configuració o parametrització del software.

A més, es considerarà incidència qualsevol incident de seguretat (confidencialitat, integritat i disponibilitat) que afecti al sistema d'informació i/o a les dades de caràcter personal, considerant incloses dins dels incidents de seguretat en l'eix de disponibilitat les còpies fallides o la impossibilitat de restauració.

Per tant, l'empresa contractista haurà de resoldre qualsevol incidència durant l'execució del contracte, així com, les consultes que es puguin produir en l'àmbit tecnològic.
Les incidències detectades per la DSTSC es faran arribar categoritzades al contractista, a través de l'eina de gestió homologada en tot moment per la DSTSC.

Serà responsabilitat de l'empresa: l'anàlisi de la incidència, proposar solucions, implementar la solució acordada amb la DSTSC.

Davant els incidents de seguretat, el contractista ha de tenir en compte:

- La classificació dels incidents de seguretat es farà segons indica la guia CCNSTIC 817, tenint el contractista la obligació de comunicar a la Diputació de Barcelona de forma immediata tots aquells que puguin ser classificats L3-Nivell Alt o superior per la via que determina el contracte.

- Respecte a les violacions de seguretat de dades de caràcter personal, l'empresa contractista haurà de tenir en compte, la clàusula 2.19 del PCAP, sobre la seva comunicació sense dilació indeguda.

L'empresa contractista tractarà els incidents de seguretat com a incidències i els classificarà segons la guia CCN-STIC 817. Els incidents de nivell L3-Nivell Alt es comunicaran de forma immediata a Diputació de Barcelona.

Una incidència estarà resolta, si està plenament documentada i té el vistiplau funcional i tècnic de la DSTSC. Tota incidència resolta per l'empresa contractista que no rebi el vistiplau de la DSTSC serà retornada a l'empresa contractista acumulant els temps de resolució.

La DSTSC treballarà conjuntament amb l'empresa contractista per reduir el temps de resolució, ja sigui proporcionant informació, fent proves o a través de qualsevol altre acció que estigui al seu abast.

5.4. Horari del suport tècnic

El contractista proporcionarà un suport tècnic en horari d'atenció de 9 h a 17h, de dilluns a divendres, no festius, a la ciutat de Barcelona.

5.5. Canals de comunicació

La DSTSC utilitza com a eina de seguiment de les peticions el Service Desk de PROLIN. La comunicació d'incidències o de peticions es realitzarà, a partir d'aquesta eina, a l'empresa contractista que rebrà un correu electrònic.

Qualsevol canvi de situació de la incidència o petició que faci l'empresa contractista ha de quedar reflectit en el Service Desk.

En el cas d'incidències critiques o urgents, s'utilitzarà el telèfon en primera instància, que haurà d'estar disponible 24x7 i utilitzant el català o castellà com a llengua. Posteriorment, la petició s'anotarà també en el Service Desk.

Si l'empresa contractista utilitza una eina pròpia per a la gestió interna de les tasques es facilitarà la integració. Si la integració amb l'eina de l'empresa contractista no és possible, la DSTSC proporcionarà un usuari d'accés al seu sistema amb l'únic objectiu de garantir l'actualització de les dades. En qualsevol cas la gestió del compliment d'ANS serà a càrrec del contractista i no es podrà obtenir a partir del sistema de la DSTSC.

5.6. Seguiment del contracte

El contractista farà un informe trimestral en relació a l'execució del contracte, on figurarà l'evolució de totes les actuacions realitzades. Aquest informe estarà a disposició de la DSTSC, abans del 10è dia de l'inici de cada trimestre posterior, al que s'està avaluant.

A continuació es detalla la informació que haurà de constar (com a mínim) en aquest informe de seguiment del contracte:

Dades del suport:

- Volumetria servei:
  - Nombre d'usuaris Microsoft 365 copiats en el període.
  - Restauracions realitzades.
  - Dades de configuració de les copies: retenció i periodicitat.

- Gestió d'incidències:
  - Quadre resum del període, amb el nombre d'incidències tractades, agrupades per categoria i nivell.
  - Situació detallada de les incidències escalades. Per a cadascuna de les incidències l'estat, informació de la situació, activitats que s'estan desenvolupant per resoldre-les i planificació de la seva resolució.
  - Quadre de compliment d'ANS per categoria. El % de compliment es realitza a partir del següent algoritme:

Total Incidències dins l'ANS / Total incidències

Computaran com a "total incidències" les que hagin estan en situació de tractament per part de la contractista en el mes. Computaran com a "total incidències dins l'ANS" el "total incidències" que estiguin dins dels terminis de compliments dels ANS.

En aquesta secció es detallaran les incidències que d'acord amb la DSTSC, es consideri que, per diferents motius, no han de ser incloses en aquest còmput.

Resum dades monitoratge:

- Temps de disponibilitat de la plataforma.
- Alarmes generades per tipologia.
- Dades de la Gestió de la capacitat: nombre usuaris, rendiment, etc.
- Gràfiques d'evolució.
- Llista d'alarmes esdevingudes durant el període.
- Propostes d'evolució de la plataforma.

Dades gestió:

- Estat d'accions de millora del servei.
- Situació econòmica del contracte, indicant les factures presentades.

Si els tècnics de la DSTSC ho consideren necessari, s'organitzaran reunions de seguiment, per tal de treballar per a la millora constant de la prestació. A aquestes reunions hi assistirà per part de l'empresa contractista el responsable del contracte. En aquestes reunions es revisaran els informes trimestrals, el funcionament dels processos, es definiran propostes de millora i es farà un seguiment de tot allò relacionat amb el contracte. L'acta de la reunió anirà a càrrec de l'empresa contractista.

La DSTSC podrà demanar informes puntuals sobre problemes, incidències, canvis, propostes de millora, etc. Així mateix, la DSTSC podrà convocar a l'empresa contractista per reunions puntuals sobre temes específics o reunions operatives.

En relació a les reunions a realitzar durant el termini de vigència del contracte, sigui quina sigui la seva periodicitat i motiu de la seva convocatòria, es podran realitzar tant en modalitat presencial com telemàtica, sempre a criteri dels tècnics de la DSTSC. La contractista disposarà dels mitjans necessaris per tal d'adequar-se a qualsevol dels formats, sense que això generi cap cost addicional per a la Diputació de Barcelona.

5.7. Equip de treball

En relació als integrants de l'equip de treball que l'empresa contractista ha de disposar a la seva plantilla per a la prestació del contracte, amb independència del seu percentatge de dedicació final, s'hauran de correspondre amb els perfils següents:

- Responsable del contracte.

  Realitzarà les tasques de coordinació, seguiment i control de la gestió del contracte. Per part de la DSTSC es designarà una persona que realitzarà funcions anàlogues.

  Serà funció del responsable del contracte de l'empresa contractista conèixer en profunditat les prestacions cobertes i assegurar que tot el personal de l'empresa contractista que participa en el contracte tingui els coneixements adients i assumeixi els compromisos adquirits i vetlli pel compliment de tots els requeriments inclosos en el contracte.

  Les principals funcions del responsable del contracte són:

  - Coordinació, seguiment, control de la gestió i qualitat del servei i amb qui es treballarà per fixar i revisar l'execució del contracte. Per part de la Diputació de Barcelona, la DSTSC designarà un coordinador que realitzarà les funcions anàlogues.

  - Supervisió de la posada en marxa per a complir amb el pla presentat, d'acord amb els requisits que determini el coordinador de la DSTSC.

  - Supervisió dels incidents, problemes, consultes, peticions, etc.

  - Gestió de l'escalat. Els incidents (o qualsevol altra acció) que necessitin ser escalats a recursos tècnics o a nivells de responsabilitat superiors dins de la pròpia empresa o en el cas de subcontractació a altres empreses, seran gestionats estretament per accelerar la seva resolució.

  L'empresa contractista haurà d'estar en disposició de donar cobertura immediata en cas de malaltia, vacances o qualsevol altra contingència que afecti el seu personal, a fi que en cap supòsit la prestació resti sense cobrir.

6. Prova de concepte

La Diputació de Barcelona, a través de la DSTSC, es reserva el dret a demanar a les empreses licitadores (inicialment a la que s'hagi proposat com a adjudicatària), sense cost addicional, la realització d'una prova de concepte, per tal de validar que la solució tecnològica proposada s'ajusta a les funcionalitats que s'han recollit en aquest plec de prescripcions tècniques.

L'empresa adjudicatària s'encarregarà de preparar a les seves instal·lacions el seu producte i facilitar l'accés als tècnics que determini la DSTSC, de manera que des d'un lloc de treball corporatiu, que tingui instal·lada la maqueta estàndard corporativa, es pugui realitzar la dita comprovació.

Per a la realització de la prova de concepte, els tècnics de la DSTSC proporcionaran a l'empresa proposada com a adjudicatària:

- Una adreça IP pública de la Diputació de Barcelona, la qual ha de ser l'única adreça IP permesa per accedir al gestor d'administració de l'eina, i des de la qual s'efectuarà aquesta prova de concepte.

- Les dades necessàries per a què l'eina de còpia de seguretat proposada es pugui connectar a la plataforma Microsoft 365 de la Diputació de Barcelona per a poder efectuar còpies de seguretat i restauracions.

- 3 usuaris del directori actiu de la infraestructura de la Diputació de Barcelona per a què puguin accedir a l'eina, cadascun amb els rols que es detallen a continuació.

- 4 usuaris amb llicència Microsoft 365 sobre els quals s'efectuaran les proves de còpia de seguretat i restauració. Durant la prova de concepte, es crearà un cinquè usuari per a verificar que és afegit a les polítiques de backup de manera automàtica i desatesa. També, es facilitarà una bústia departamental, la qual s'haurà de copiar.

Aquesta prova es farà amb el suport de la DSTSC i amb els referents del Servei de Gestió d'Operacions TIC, a partir d'una validació bàsica que permeti:

1. Validar que el gestor d'administració de l'eina només pot ser accedit des de l'adreça IP proporcionada per la Diputació de Barcelona. Es validarà que l'accés des d'altres adreces IP a aquesta pàgina web és denegat i no permet ni tan sols introduir un usuari i contrasenya, per així evitar intents d'accés per força bruta.

2. Validar que l'accés a l'eina és possible des dels navegadors de la maqueta estàndard de la Diputació de Barcelona sense necessitat d'instal·lar cap complement o cap programa que no estigui instal·lat per defecte a la maqueta.

3. Validar que l'eina permet la validació dels usuaris donats d'alta amb les seves contrasenyes del directori actiu. També, es validarà l'accés a l'eina amb l'usuari local d'aquesta, segons l'especificat al paràgraf 4.2 dels "Requeriments funcionals".

4. Assignar als 3 usuaris creats, els rols de creació de polítiques de còpies, de recuperació i de visualització del log i creació de nous usuaris i rols, respectivament, a fi de validar que cada usuari disposa només dels seus permisos.

5. Efectuar backup de les dades (bústia d'Exchange, dades de Sharepoint, de OneDrive i conversa de Teams) dels 4 usuaris, així com de la bústia departamental.

6. Crear a Microsoft 365 un cinquè usuari i validar que és afegit a la política de còpia de seguretat de manera desatesa, sense cap acció per part dels usuaris que efectuen la prova de concepte, segons el detallat en el present plec al paràgraf "Autodescobriment d'usuaris Microsoft 365".

7. Configurar còpies de seguretat per verificar el punt "Configuració de la planificació i la retenció". Efectuar també una còpia "on demand".

8. Un cop efectuades les còpies de seguretat es validarà el cercador de documents.

9. Efectuar una restauració granular d'un element d'una bústia sobre la mateixa bústia, sobre una altra i a disc. Posteriorment, s'eliminarà una bústia i es restaurarà aquesta de manera total.

10. Efectuar restauració d'un fitxer de OneDrive i d'elements de Teams.

11. Un cop efectuades les validacions dels punts anteriors, es comprovarà l'existència del log de moviments i la gravació dels esdeveniments detallats al present plec de les proves fetes anteriorment.

Es considerarà que la solució tecnològica proposada té l'acceptació de la DSTSC, si es constata que els resultats de la prova de concepte han permès garantir, de manera objectiva, que la solució proposada ha complert amb les especificacions tècniques i els criteris de validació inclosos a la prova de concepte i detallats en els paràgrafs precedents d'aquest mateix apartat.

7. Posada en marxa

La posada en marxa és el període de temps que transcorre entre l'inici de l'execució del contracte i l'assoliment dels nivells de servei fixats en aquest Plec de prescripcions tècniques. En aquesta fase, el contractista posarà en marxa els procediments i eines necessàries per a l'execució del servei, i els integrarà amb els procediments, processos i eines existents a la DSTSC.

La DSTSC assignarà un interlocutor que treballarà conjuntament amb l'empresa contractista en la fase de posada en marxa.

Serà responsabilitat del contractista l'execució de les diferents tasques que conformen la posada en marxa de la solució.

Durant la primera reunió de treball, l'empresa contractista haurà de presentar el pla de posada en marxa, que ha d'incloure els mecanismes necessaris per executar tota la posada en marxa de la solució: traspàs de coneixement, reunions, connectivitat a l'entorn, presentació de recursos assignats i concreció de protocols d'actuació.

Per a la posada en marxa de la solució, l'empresa contractista disposarà d'un termini d'execució de 30 dies naturals o inferior si es millora en l'oferta, comptadors a partir de. la data d'activació de les llicències backup i restore O365 . A partir d'aquest moment, s'aplicaran les penalitats corresponents.

Formen part de la prestació, les activitats, d'implementació i formació als usuaris de la corporació, prèvies a la posada en marxa per assegurar el correcte funcionament del sistema, d'acord amb les especificacions detallades (tant tècniques com funcionals).

Així mateix, forma part del procés d'implementació la connexió de la solució de backup al núvol amb la infraestructura Microsoft 365 de la Diputació de Barcelona, mitjançant un usuari i contrasenya i una primera configuració de les polítiques de còpies de seguretat segons les especificacions dels tècnics de la DSTSC.

Les còpies de seguretat han de començar a realitzar-se passat el termini de 30 dies naturals dedicats a la posada en marxa de la solució. Un cop configurada la solució i dins del termini màxim fixat per a la seva posada en marxa, l'empresa contractista realitzarà una formació per tal de traspassar el servei als tècnics que la DSTSC indiqui.

L'objectiu d'aquesta formació és que els tècnics de la DSTSC adquireixin el coneixement necessari perquè puguin administrar la solució de manera autònoma i fer-la evolucionar segons els interessos propis de la DSTSC. La formació consistirà en una jornada de 8 hores i es realitzarà de manera telemàtica. En aquesta formació s'haurà de traspassar el coneixement, com a mínim, dels següents punts:

- Accés a la solució.
- Creació, modificació i eliminació de polítiques de còpies de seguretat.
- Verificació de les còpies de seguretat.
- Realització de còpies de seguretat sota demanda (manualment).
- Realització de restauracions dels diferents productes de Microsoft 365.
- Configuració d'alertes de backups finalitzats, fallits i no inicialitzats, així com d'esdeveniments de la solució.
- Creació i configuració d'usuaris a la solució i aplicació dels diferents rols.
- Consultes dels logs de registre.

El cost que impliqui o que es derivi de qualsevol de les actuacions derivades de la posada en marxa, s'ha d'entendre inclòs en el pressupost total del contracte.

8. Acords de Nivell de Servei (ANS)

Els ANS permeten obtenir indicadors per avaluar el grau de compliment del contracte.

El càlcul de l'ANS es realitzarà amb una periodicitat mensual i considerant l'horari de la prestació i el mes natural.

No computaran els períodes de temps en que el contractista està pendent de resposta, reunions, dades o concreció de requeriments per part dels tècnics o usuaris de la Diputació de Barcelona o de tercers proveïdors sempre i quan, aquests no tinguin una relació contractual directa amb l'empresa contractista principal, donat que en aquell cas el temps computarà com a temps propi del contractista a tots els efectes previstos en aquest Plec.

8.1. ANS de resolució d'Incidències

Les incidències només es consideraran finalitzades si es troben completament documentades i tenen el vistiplau funcional i tècnic de la DSTSC, en cas contrari seran retornades a l'empresa contractista acumulant els temps de resolució, a tots els efectes i responsabilitats establertes en l'ANS corresponent.

Temps de resposta: és el temps transcorregut entre la comunicació de la incidència a l'empresa contractista pel canal previst fins que aquesta l'assumeix assignant els recursos necessaris per a poder complir el temps de resolució.

Temps de resolució: és el temps transcorregut entre la comunicació de la incidència a la contractista pel canal previst, fins que la incidència queda resolta i documentada per l'empresa contractista.

S'estableixen quatre categories d'incidències, amb diferents ANS, pel temps de resolució (els temps són sempre dins de l'horari de servei, per tant, sempre computat sobre hores, dies o períodes de dies naturals):

Indicadors per a la gestió d'incidències	Temps de resolució
A1. Crítica. Incidències que suposen no accedir a la solució o afecten de manera molt global a tot el sistema de còpies. Incidents de seguretat nivell Alt.	4 hores
A2. Urgent. Incidències que suposen l'aturada d'alguna funcionalitat bàsica.	24 hores
A3. Important. Incidències que afecten a una funcionalitat amb impacte limitat.	5 dies
A4. Estàndard. Incidències que no aturen l'operativa diària.	10 dies

8.2. ANS de la disponibilitat del servei de suport

L'empresa contractista haurà de garantir la disponibilitat del servei de suport. En cas d'indisponibilitat, el temps de resolució serà de 2 hores.

9. Transició del servei

La fase de transició del servei només s'activarà, en el cas que hi hagi alternança entre contractistes.

Aquesta fase de transició del servei s'estableix entre el moment en que la nova empresa es fa càrrec del servei de còpies de seguretat i restauracions i l'expiració de les còpies de seguretat de l'empresa sortint, amb una durada d'un any.

Donat el gran volum d'informació previst de les còpies de seguretat emmagatzemades durant la vigència del contracte, així com pel format propietari de les còpies (que impossibilitaran una possible exportació), i amb l'objectiu de garantir la restauració d'aquelles còpies que no hagin arribat al final del seu període d'expiració, durant aquesta fase de transició, l'empresa sortint no efectuarà més còpies i únicament permetrà restaurar les còpies de seguretat existents al núvol (amb la mateixa granularitat i funcionalitats que en la resta del contracte), mentre que la nova empresa contractista efectuarà còpies de seguretat de l'entorn Microsoft 365 i permetrà la restauració de les noves dades durant la vigència del nou contracte.

En aquest sentit, l'empresa contractista s'haurà de comprometre a realitzar una bona gestió i seguiment dels serveis objecte d'aquest contracte, garantint-ne la prestació continuada en el temps, segons els acords de nivell de serveis i amb lliuraments de

qualitat, així com assegurar el traspàs d'informació (procediments de gestió, dades i documents) i coneixement entre contractistes en la fase de transició del servei.

Quan hi hagi continuïtat de contractista aquesta haurà de lliurar a la DSTSC una memòria tècnica explicativa proposant millores, si escau, en la prestació del servei.

10. Devolució del servei

Un cop finalitzada la fase de còpies i restauracions, el contractista haurà de permetre la descàrrega de tots els logs de moviments disponibles en aquell moment a la solució. El format d'aquest log haurà de ser en text pla i amb els camps delimitats per a poder ser importat a altres aplicatius d'anàlisi, com Excel.

Els objectius seran:
- Recollir el traspàs de coneixement per part del contractista sortint amb la finalitat de garantir la continuïtat del servei.
- Recollida acurada de requeriments per a la planificació de l'arrancada del servei per part del contractista alternatiu.
- Preparació i proves dels accessos remots al sistema d'informació, per a la seva disponibilitat el dia d'inici de la prestació efectiva del servei.
- Preparació dels entorns necessaris per a la prestació adequada del servei.

A més, la contractista haurà de garantir, mitjançant un document, que ha destruït de manera efectiva, i sense que es puguin recuperar de cap manera, la totalitat de les dades de les còpies de seguretat que estiguin desades al sistema d'emmagatzematge al núvol sobre el qual ha prestat el servei durant la vigència del contracte.

Així mateix, el document haurà d'acreditar que la contractista ha desconfigurat i inhabilitat la connexió existent contra la plataforma de Microsoft 365 de la Diputació de Barcelona, de manera que sigui impossible accedir a cap informació existent a la plataforma ni als usuaris o contrasenyes del directori actiu de la Diputació de Barcelona.

11. Transferència tecnològica i de coneixement

La contractista està obligada a facilitar a les persones designades per la DSTSC tota aquella informació necessària per disposar d'un ple coneixement tècnic de les prestacions realitzades.
Tanmateix, el personal tècnic designat per la DSTSC per a fer gestió de les prestacions contractades, podrà realitzar totes aquelles consultes que consideri oportunes per al correcte seguiment i control del contracte, com també, rebent, si escau, el traspàs de la informació que sigui necessària per a conèixer i comprendre el funcionament dels mateixos.

Metadades del document

Núm. expedient	2026/0004487
Tipus documental	Plec de clàusules o condicions
Títol	Plec de prescripcions tècniques particulars relatiu a la contractació d'una solució integral (SaaS) de gestió de la còpia de seguretat i restauració, al núvol, de la plataforma Microsoft 365 de la Diputació de Barcelona
Codi classificació	3107 - Contractacions de subministraments per procediment obert subjecte a regulació harmonitzada

Signatures

Signatari		Acte	Data acte
Francisco Javier Gimenez Bruque(TCAT)	Responsable directiu Servei Promotor	Signa	08/05/2026, 16:06

Validació Electrònica del document

Codi (CSV)	Adreça de validació	QR
24975c8cc74be161d11f	https://seuelectronica.diba.cat	