Área de Servicios Generales y Transición Digital
Dirección de Servicios de Tecnologías y Sistemas Corporativos

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DE UNA SOLUCIÓN INTEGRAL (SaaS)DE GESTIÓN DE LA COPIA DE SEGURIDAD Y RESTAURACIÓN, EN LA NUBE, DE LA PLATAFORMA MICROSOFT 365 DE LA DIPUTACIÓN DE BARCELONA

Exp. 2026/0004487

Índice

1. Antecedentes

La Dirección de Servicios de Tecnologías y Sistemas Corporativos (DSTSC) de la Diputación de Barcelona tiene como misión proporcionar todos los servicios e infraestructuras de informática y telecomunicaciones de la Diputación de Barcelona, en el ámbito interno y también dar soporte a los entes locales, estableciendo estrategias de futuro alineadas con las necesidades funcionales corporativas y optimizando la relación coste-beneficio.

Los servicios de tecnologías y sistemas corporativos se entienden como la integración de los ámbitos clásicos de la informática y las telecomunicaciones. Se asegura una dirección única para el tratamiento lógico de la información y sus redes de transmisión, independientemente de su formato físico (voz, datos o imagen).

Las funciones asignadas a la DSTSC son:

- Realizar los criterios fijados por la Diputación de Barcelona en materia de tecnologías de la información (en adelante TIC). Es decir, informática, telecomunicaciones y, en general, aquellas tecnologías relacionadas con el tratamiento automatizado de la información, y proponer los recursos necesarios a habilitar para este fin.
- Coordinar las tareas administrativas de TIC de todas las unidades de la Diputación de Barcelona y, de forma particular, las que tienen interrelación, y proponer las medidas adecuadas para una máxima normalización.
- Controlar y realizar el seguimiento de aquellas tareas en materia TIC realizadas por la Diputación de Barcelona mediante recursos externos.
- Proponer y gestionar las actuaciones a desarrollar por la Diputación de Barcelona en materia TIC que, dentro de los supuestos de la cooperación y asistencia, se realicen para los entes locales de la provincia de Barcelona.
- Desarrollar y gestionar los proyectos en TIC que se produzcan a propuesta de las áreas, direcciones y servicios de la Diputación de Barcelona.
- Coordinar la formación y el reciclaje del personal de la Diputación de Barcelona en materia TIC.
- Informar del gasto económico que generen las áreas, direcciones y servicios de la Diputación de Barcelona y sus organismos autónomos en materia TIC.
- Asesorar a los organismos autónomos de la Diputación de Barcelona en materia TIC, cuando así se requiera y tutelar, si procede, la homogeneidad en el tratamiento de los sistemas de información comunes.
  Prestar apoyo para la adecuación corporativa al cumplimiento de la normativa de protección de datos y del Esquema Nacional de Seguridad, en los aspectos jurídicos, organizativos y tecnológicos de los tratamientos realizados por la Diputación de Barcelona, no sólo como responsable de este tratamiento para los entes locales sino también como encargada.

Por lo que respecta al objeto específico de este expediente, la DSTSC utiliza Microsoft 365 para los empleados de la Diputación de Barcelona, de algunos ayuntamientos y de los trabajadores de la Red de Bibliotecas de la Diputación.

Todos los datos que los usuarios almacenan en cualquiera de las utilidades del entorno Microsoft 365 (Outlook -Exchange online-, Share Point, Microsoft Teams, OneDrive y Groups) se almacenan en los repositorios de Microsoft en la nube.

Para garantizar completamente la disponibilidad ante cualquier ataque, paro o incidente de los datos en la nube, así como para adaptar el servicio a las políticas de copia y restauración aprobadas por la Diputación de Barcelona, la DSTSC considera necesario disponer de una copia de los datos fuera del entorno Microsoft 365 y fuera del entorno corporativo.

En concreto:

- Adaptar los tiempos de retención de las copias de seguridad, a los criterios que considere más adecuadas la DSTSC.
- Adaptar los criterios de granularidad de la restauración de los datos a las necesidades de la DSTSC.

2. Objeto

Es objeto del presente pliego definir las especificaciones técnicas particulares para la contratación de una solución integral de gestión de la copia de seguridad y restauración, en la nube, de la plataforma Microsoft 365 de la Diputación de Barcelona.

3. Alcance

La empresa contratista deberá proporcionar una solución integral, con todos los elementos necesarios para la prestación del servicio (entendido como una solución completa e integrada) que incluya la capacidad de copiar y restaurar, según las especificaciones y requerimientos establecidos en el presente Pliego, de todos los datos generados en la plataforma Microsoft 365 de la Diputación de Barcelona, en cuanto a los usuarios licenciados, así como, todo el servicio de infraestructura y sistemas de base (en sentido amplio) necesarios para la correcta prestación del servicio. Los datos para copiar y restaurar serán, como mínimo, los de las siguientes aplicaciones incluidas dentro de la plataforma Microsoft 365:

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

La empresa contratista deberá dimensionar la infraestructura y los sistemas de base necesarios para la prestación del servicio, proporcionando la capacidad de procesamiento y el espacio de almacenamiento suficiente para guardar todas las copias generadas con la retención definida por la DSTSC, durante la totalidad de la vigencia del contrato. La capacidad de almacenamiento de la solución deberá ser suficiente para poder alojar las copias de seguridad con la retención definida por la DSTSC.

En caso de que deba incrementarse de este dimensionamiento, no representará ningún coste adicional para la Diputación de Barcelona.

En ningún caso, el coste del contrato se verá afectado por el volumen de datos transmitidos al servicio de copias y restauración.

La empresa contratista también aportará todo el software y las herramientas de seguridad necesarias para garantizar la privacidad de los datos.

4. Descripción del contrato

El contratista deberá proveer una solución completa e integrada de copia de seguridad y restauración, para mantener las copias de todos los datos generados por el uso de las aplicaciones de Microsoft 365 en la nube de Microsoft, para todos los usuarios que disponen de licencias en la Diputación de Barcelona.

La Diputación de Barcelona podrá decidir cada cuánto tiempo se realiza la copia de los datos y durante cuánto tiempo se mantiene la retención de cada una de las copias. Los técnicos de la DSTSC serán los únicos que accedan a las copias para restaurar los datos necesarios y realizarán las tareas de administración de la solución.

El servicio contratado estará formado por dos fases: la primera fase, con una vigencia de 3 años, corresponde a la realización de copias de seguridad y restauraciones con la modalidad de licencia backup (copia) y restore (restauración) M365 (cl. 4 y 5 de este Pliego); y una segunda fase, con una vigencia de un año y que sólo se activará en caso de que exista alternancia entre contratistas, a la que se realizarán únicamente restauraciones, con el objetivo de poder restaurar en cualquier momento, si se necesita, las copias no expiradas (cl. 9 de este Pliego). La modalidad de licencia aplicable a la segunda fase será exclusivamente la de Licencia Restore M365.

La empresa licitadora propuesta como adjudicataria, en los plazos que prevé la cláusula 1.18 del Pliego de cláusulas administrativas particulares, deberá acreditar, antes de la adjudicación, que cumple con los siguientes requisitos:

Certificación Élite, Gold o equivalente de la empresa fabricante del software propuesto.

4.1. Requerimientos funcionales

En este apartado se describen los requerimientos funcionales que debe cumplir la solución, en concreto:

- **Acceso al software de gestión a través de un navegador web**
  Para acceder a cualquier funcionalidad de gestión se realizará a través de un navegador web. No será necesaria, la instalación de ningún software en el equipo de la persona que acceda al mismo.

- **Autenticación de usuarios**
  La solución no almacenará ningún usuario, ni contraseña. La validación de los usuarios se realizará mediante el estándar SAML con la herramienta de gestión de identidades de la DSTSC. Únicamente existirá un usuario local en el sistema, que se utilizará en caso de que el sistema de gestión de identidades de la DSTSC esté fuera de servicio.

  El sistema debe permitir limitar las direcciones IP desde donde se conectan los usuarios a la solución y bloquear el acceso desde el resto de las direcciones IP no autorizadas por la DSTSC.

- **Log de movimientos**
  El sistema dispondrá de un log donde quedarán registrados, como mínimo, los siguientes eventos:

    - Fecha, hora y usuario de los accesos válidos.
    - Fecha, hora y usuario de los intentos de acceso no válidos.
    - Fecha, hora y usuario de las creaciones, modificaciones o eliminaciones de políticas de copias de seguridad.
    - Fecha, hora, usuario y descripción de los datos recuperados de la copia de seguridad.

- **Control de acceso basado en roles**
  La solución debe permitir la asignación de diferentes roles a los usuarios autorizados para poder interactuar con ellos, siempre bajo la premisa del principio del mínimo privilegio. Al menos, deberá permitir asignar los siguientes roles:

    - Configurar copias de seguridad.
    - Recuperar copias de seguridad (sin poder ver el contenido de los correos y archivos de las copias de seguridad).

- Recuperar copias de seguridad (pudiendo ver el contenido de los correos y archivos de las copias de seguridad).
- Visualizar el log de registro.
- Recuperar copias de seguridad de usuarios marcados con la funcionalidad “Derecho de ser olvidados”.
- Añadir/eliminar/modificar usuarios y roles.

- **Productos de Microsoft 365 cubiertos por la solución**
  La solución de copia de seguridad debe poder proteger y recuperar (en la misma ubicación y en una ubicación alternativa), como mínimo, los siguientes elementos de Microsoft 365:

  - Microsoft Exchange:
    - Buzones de correo electrónico de los usuarios.
    - Buzones departamentales o grupales.
    - Carpetas Públicas.
    - Calendarios.
    - Contactos.

  - SharePoint:
    - Archivos.
    - Versiones de los archivos.
    - Directorios.
    - Bibliotecas.
    - Listas y elementos de listas.
    - Sitios Teams y subsitios.
    - Notebooks.
    - Páginas.
    - Permisos.
    - Formularios.
    - Plantillas.

  - OneDrive:
    - Archivos.
    - Versiones de los archivos.
    - Directorios.

  - Teams:
    - Teams de equipos públicos, privados y de toda la organización.

- Channels de canales regulares y privados.
- Tabs de publicaciones, archivos, wiki, sitios web, Word, Excel, PowerPoint y PDF, bibliotecas de documentos, nombres, tipos y ajuste de pestañas.
- Conversaciones y post (elementos de las conversaciones y las respuestas).
- Calendarios.
- Archivos.

- Grupos:
  - Grupos creados en Yammer, Planner y Outlook.

- Identidades y objetos Microsoft Entra ID:
  - La solución deberá ser capaz de efectuar copias de seguridad de objetos de identidades y accesos disponibles en Microsoft Entra ID, incluyendo, como mínimo:
    - Usuarios.
    - Grupos.
    - Roles.
    - Logs de actividad.
    - Unidades administrativas.
    - Claves de cifrado Bitlocker.

La restauración de estos objetos deberá poder efectuarse sobre la misma nube de Microsoft ya una ubicación alternativa.

- **Autodescubrimiento de usuarios Microsoft 365**
  La solución deberá auto descubrir a los nuevos usuarios de la plataforma Microsoft 365 de la Diputación de Barcelona, no requiriendo ninguna intervención manual por parte de los técnicos para añadir un nuevo usuario (de cualquiera de las aplicaciones incluidas en el apartado Alcance del presente Pliego). La solución la añadirá a la copia de seguridad de forma automática. Esta funcionalidad deberá permitir configurar a los usuarios a copiar a través de grupos de Active Directory.

- **Configuración de la planificación y la retención**
  La solución permitirá efectuar, de forma automática y desatendida, como mínimo, una copia de seguridad al día. También, deberá permitir efectuar copias “on demand”.

  El sistema deberá permitir configurar la retención de cada copia, limitando el período de retención de cada una de ellas. La retención mínima será de un año y

deberá ser ampliable hasta 3 años, sin que ello suponga ningún coste adicional para la Diputación de Barcelona.

- **Buscador de documentos**
  Dispondrá de un buscador que permita localizar documentos, dentro de los backups, a fin de facilitar las tareas de búsqueda y filtrado para localizar la información, canales de conversaciones, archivos, Teams o correos electrónicos a restaurar. El buscador deberá permitir la indexación para localizar los datos de forma ágil, independientemente del número de copias retenidas.

- **Derecho al olvido**
  Con el objetivo de cumplir con el GDRP, la solución debe disponer de la capacidad de marcar copias de seguridad con una funcionalidad que permita identificar y bloquear información, a fin de evitar que se pueda restaurar de forma estándar, también conocida como derecho al olvido o right to be forgotten.

  Cuando una información de copias de seguridad de un usuario se identifique con esta característica, estos datos sólo podrán ser restaurados por un usuario con derechos elevados distinto a los usuarios que restauran de forma ordinaria.

Tipo de restauraciones permitidas por la solución

La solución de copia de seguridad permitirá restaurar, como mínimo, los siguientes elementos con la siguiente granularidad:

- Microsoft Exchange:
  - Restaurar un buzón completo, incluyendo correos, calendarios y contactos.
  - Restaurar correos, calendarios y contactos de forma granular en un archivo PST o archivos independientes (.eml, ics, vcf...), en el buzón origen y en un buzón diferente.
  - Restaurar datos de buzones eliminados.
  - Objetos eliminados.

- SharePoint:
  - Sites.
  - Archivos, incluyendo archivos de tamaño superior a 2 GB.
  - Sitios de nivel superior (Top-level site) y sub-sites.
  - Documentos, elementos de lista y bibliotecas eliminadas.

- La restauración debe poder efectuarse en el sitio original o en otros sites.

- OneDrive:
  - Archivos.
  - Versiones de los archivos.
  - Directorios.
  - Cuentas OneDrive

- Teams:
  - Restauración de los elementos especificados en el apartado anterior que describe los elementos cubiertos por la solución de Teams.

- EntraID:
  - Restauración de los elementos especificados en el apartado anterior que describe los elementos cubiertos por la solución de EntraID.

La herramienta deberá disponer de una funcionalidad para crear una dirección URL única que permita, una vez validado un usuario con una contraseña, acceder a la herramienta de backup, sólo a los datos configurados para recuperar, para que el propio usuario pueda efectuar la restauración de los datos. La herramienta deberá permitir configurar una fecha de expiración de esta URL.

El número de restauraciones a realizar será ilimitado, sin que ello suponga coste adicional alguno para la Diputación de Barcelona.

Soporte multi-tenant

El entorno Microsoft 365 de la Diputación de Barcelona está formado por multitud de tenantes. Esto significa que la solución debe poder soportar el funcionamiento multi-tenant, garantizando que la capacidad del almacenamiento es la suficiente para efectuar los backups de todos los datos, ficheros y buzones creados en los diferentes tenantes y las retenciones que la DSTSC establezca en las copias de seguridad, siempre respetando el número máximo de usuarios especificado en el presente pliego. La DSTSC podrá crear más tenantes para adecuarlo a su crecimiento y la solución cubrirá a los nuevos tenantes.

Los datos de los diferentes tenantes tendrán que estar aislados entre sí. El sistema deberá permitir limitar a los distintos usuarios la posibilidad o no de restaurar de los distintos tenantes, configurando los roles de acceso para cada tenante independientemente.

4.2. Requerimientos técnicos

En este apartado se describen todos los requerimientos técnicos que debe cumplir la solución, en concreto:

- **Alta disponibilidad**

  La solución debe disponer de los elementos necesarios para garantizar la disponibilidad 24x7. Para ello, es un requisito indispensable que todos los elementos necesarios para el funcionamiento del servicio (servidores, software, almacenamiento, comunicaciones y elementos de seguridad) sean redundantes. Los datos de las copias de seguridad tendrán que estar simultáneamente en dos centros de proceso de datos diferentes y georredundantes. Estos centros de datos tendrán que ser diferentes e independientes de los centros de datos de Microsoft.

- **Rendimiento**

  La solución debe garantizar que está dimensionada en todo momento para poder efectuar las copias de seguridad y las restauraciones con un rendimiento que garantice que la ejecución de cualquier copia no supere una duración de 24 horas (para asegurar que siempre exista una copia diaria de todos los datos) y que la restauración de un buzón de 10 GB no supere los 15 minutos de duración minutos. El crecimiento de los datos de copias de seguridad almacenados no podrá suponer en ningún caso una descarga del rendimiento antes indicado.

  El proceso de copia de datos no puede afectar al rendimiento del uso de la plataforma Microsoft 365.

- **Seguridad**

  La solución deberá disponer de un sistema que detecte posibles casos de Ransomware u otros tipos de ciberataques. Esta detección la efectuará analizando cambios anómalos en las copias de seguridad que realice (modificaciones, borrados, crecimientos anormales, etc.), que podrán ser indicativos de un posible ataque de Ransomware, otros tipos de ciberataques o en situación de corrupción de los datos. Cuando la solución detecte esta situación, generará una alerta para que el equipo técnico de la DSTSC lo analice.

  Todos los datos y metadatos almacenados en la copia deberán estar cifrados. El acceso a la plataforma de gestión e internamente, en el almacenamiento, se efectuará en todo momento mediante conexión HTTPS.

Debe garantizarse que los datos de las copias de seguridad serán inmutables, de forma que un atacante no pueda alterar o eliminar estas copias.

La solución debe contar con mecanismos que garanticen que la empresa contratista no pueda acceder a los datos de las copias de seguridad ni al entorno Microsoft 365 de la Diputación de Barcelona.

La empresa contratista debe disponer de un plan de respuesta a incidentes (IRP -Incidente Response Planning-) y de procedimientos de recuperación de desastres (DRP -Disaster Recovery Plans-) que deberá ser validados y revisados anualmente con los técnicos de la DSTSC.

- **Compatibilidad con otros sistemas de copias**

  El uso del sistema de copias debe permitir utilizar simultáneamente, otros sistemas de copias sobre los datos de los propios usuarios.

4.2.1. Usuarios licenciados (volumetría estimada)

Antes del inicio de cada anualidad se fijará el número de licencias a utilizar durante el siguiente año. A tal fin, los técnicos de la DSTSC proporcionarán a la contratista, un mes antes del inicio de la anualidad, la cantidad de cada tipo de licencia y los datos necesarios para la activación.

El número de licencias podrá aumentar o disminuir según las necesidades de la Diputación de Barcelona.

La siguiente tabla detalla una estimación sobre el número de licencias activas, al inicio de cada anualidad prevista, de vigencia del contrato.

Fase de copias y restauraciones	Primer año	28.810 licencias
	Segundo año	30.110 licencias
	Tercer año	31.410 licencias
Fase de transición del servicio	Cuarto año	Restauración de 31.410 licencias

La siguiente tabla detalla la estimación de licencias que se podrán añadir durante cada una de las anualidades del contrato.

Primer año	1.300 licencias
Segundo año	1.300 licencias
Tercer año	1.300 licencias

4.2.2. Gestión de la monitorización

El sistema dispondrá de un sistema de monitorización que informará, mediante correo electrónico configurable por los técnicos de la DSTSC, de los eventos principales acaecidos, como las copias efectuadas, las copias fallidas e incidentes de funcionamiento de la solución de backup.

La empresa contratista deberá monitorizar la disponibilidad de todo el entorno administrado de forma ininterrumpida en modalidad 24x7. Esto implica:

- Monitorear la disponibilidad de la plataforma de backup.
- Monitorear la conexión entre la plataforma de backup y la infraestructura Microsoft 365.
- Monitorear la utilización de la plataforma detectando usos no deseados o ciberataques.
- Monitorear la capacidad del sistema y su rendimiento.

A partir de la actividad de monitorización de los sistemas, la empresa contratista aplicará alguna de las siguientes acciones:

- Notificará los eventos cuando sean detectados y actuará de inmediato (abriendo incidencia o tarea) ante cortes de servicio o ciberataques.
- Abrirá tareas de administración para actuaciones de mejora de la capacidad.
- Abrirá tareas de administración para actualización de componentes del sistema.

La monitorización debe permitir realizar una correcta gestión de la capacidad y por tanto, servirá para proponer actuaciones de forma proactiva para evitar que se produzcan caídas de rendimiento o cortes de disponibilidad. En caso de que se produzca alguna incidencia, servirá para poder actuar de forma inmediata.

4.2.3. Disponibilidad

Se solicita una disponibilidad del 99,7%.

En los casos en que deba procederse a la realización de tareas periódicas de mantenimiento, actualizaciones o mejoras en los equipos, software o infraestructuras, o de cualquier otro elemento incluido en el modelo SAAS, deberá procederse a su planificación, intentando paliar, en la medida de lo posible, cortes en el servicio que afecten a los usuarios finales de la solución.

Los trabajos programados se ejecutarán en la ventana de tiempo que menos perjuicio ocasione a los usuarios finales de la solución y, en todos los casos, deberá ser autorizada por la DSTSC.

Definición de tiempo de disponibilidad: es la suma del tiempo, en minutos, en que la solución ha estado disponible durante el período de tiempo establecido como medida (un mes natural). Por este contrato se entiende como servicio la disponibilidad de acceso por parte de los usuarios a las interfaces de consulta pública y administración y su operativa.

Definición de ratio de disponibilidad: es la relación del tiempo de disponibilidad respecto al tiempo total en minutos de un (1) mes natural.

Definición de ratio de disponibilidad mínima objetivo: es la ratio de disponibilidad mínima que se desea alcanzar y se indica en cantidad de nueves (9) de la ratio, por ejemplo, tres nuevos sería el 99,9% o cuatro nuevos sería el 99,99%.

Definición de tiempo de no disponibilidad: es la suma del tiempo en minutos en los que la solución no ha estado disponible durante el mes natural.

Definición de tiempo de no disponibilidad máximo objetivo: es el tiempo máximo de no disponibilidad que se desea alcanzar y se calcula, como diferencia de minutos, entre el tiempo total en minutos de un mes natural computando los días de 24h.

5. Modelo de prestación

5.1. Software as a Service

La prestación objeto de esta contratación deberá realizarse de acuerdo con el modelo de prestación conocido como Software as a Service (SaaS).

SaaS es una modalidad de solución donde el software y los datos relacionados se hospedan en servidores y sistemas de almacenamiento a cargo del proveedor de la solución y el acceso a los mismos se realiza a través de Internet de forma segura. Por tanto, la información, su procesamiento y los resultados del tratamiento de una determinada lógica de negocio estando hospedados en las instalaciones del contratista.

El contratista se hace cargo de toda la infraestructura, hardware y software necesario para la prestación del servicio. Es decir, de cualquier gasto derivado de la prestación de la solución: del software, tanto a nivel servidor como cliente (desarrollado o licenciado); del hardware (físico o virtual, así como cualquier tipo de licencia asociada); y de las comunicaciones adecuadas hasta la puesta a disposición de la información a través de Internet. Asimismo, se hará cargo de cualquier actuación que sea necesaria, sea

correctiva, preventiva o evolutiva, para mantener la solución con los parámetros de calidad y seguridad adecuados.

Otros requisitos que debe tener en cuenta el contratista en relación a esta modalidad son:

- La infraestructura para ofrecer la solución debe estar alojada en territorio de la UE.
- No se permite ningún tratamiento de datos personales fuera de la UE, ni siquiera para su almacenamiento, ni para la realización de copias de seguridad.

- Para todos los usuarios, todas las comunicaciones deben estar cifradas y deben contar con medidas de seguridad adecuadas para mantener la confidencialidad, disponibilidad, trazabilidad e integridad de los datos.

- Forma parte de la solución la devolución de los logs de movimientos y la destrucción de todos los datos, tanto los operativos como las copias de seguridad existentes, una vez finalizado el contrato. Todas las acciones correspondientes tendrán que estar certificadas.

- El sistema debe disponer de alta disponibilidad, tanto en lo que se refiere a la propia infraestructura, el equipamiento de red, líneas de datos, elementos de seguridad, como al suministro eléctrico y refrigeración de aire de la infraestructura.

- El contratista estará obligado a realizar, al menos, una revisión completa de hardware al año, con el fin de asegurar el perfecto funcionamiento del sistema y evitar incidencias futuras. Estas acciones tendrán que estar certificadas.

En ningún caso, la Diputación de Barcelona se hará cargo de los costes del almacenamiento necesario para garantizar una retención de las copias ni del tráfico de red (ni de copias ni de descarga en las restauraciones) durante toda la vigencia del contrato, estos gastos irán a cargo de la empresa contratista.

5.2. Formación

El contratista garantizará la formación actualizada en el uso del sistema de copias durante
toda la duración del contrato.

El contratista dedicará al menos dos horas mensuales a temas de formación continua en el uso de la herramienta, siempre bajo demanda de los técnicos de la DSTSC. Este tiempo también servirá, en su caso, para resolver dudas técnicas y funcionales que surjan a raíz del uso del sistema.

5.3. Gestión de las incidencias

Se trata de aquellas actuaciones que tienen como objetivo resolver disfunciones en el funcionamiento de la solución contratada y que tienden a minimizar el número de incidencias y su resolución, en el menor tiempo posible, incluso si se derivan de la configuración o parametrización del software.

Además, se considerará incidencia cualquier incidente de seguridad (confidencialidad, integridad y disponibilidad) que afecte al sistema de información y/oa los datos de carácter personal, considerando incluidas dentro de los incidentes de seguridad en el eje de disponibilidad las copias fallidas o la imposibilidad de restauración.

Por tanto, la empresa contratista deberá resolver cualquier incidencia durante la ejecución del contrato, así como, las consultas que se puedan producir en el ámbito tecnológico.
Las incidencias detectadas por la DSTSC se harán llegar categorizadas al contratista, a través de la herramienta de gestión homologada en todo momento por la DSTSC.

Será responsabilidad de la empresa: el análisis de la incidencia, proponer soluciones, implementar la solución acordada con la DSTSC.

Ante los incidentes de seguridad, el contratista debe tener en cuenta:

- La clasificación de los incidentes de seguridad se hará según indica la guía CCNSTIC 817, teniendo el contratista la obligación de comunicar a la Diputación de Barcelona de forma inmediata a todos aquellos que puedan ser clasificados L3-Nivel Alto o superior por la vía que determina el contrato.

- Respecto a las violaciones de seguridad de datos de carácter personal, la empresa contratista deberá tener en cuenta, la cláusula 2.19 del PCAP, sobre su comunicación sin dilación indebida.

La empresa contratista tratará los incidentes de seguridad como incidencias y los clasificará según la guía CCN-STIC 817. Los incidentes de nivel L3-Nivell Alt se comunicarán de forma inmediata a Diputación de Barcelona.

Una incidencia estará resuelta, si está plenamente documentada y tiene el visto bueno funcional y técnico de la DSTSC. Toda incidencia resuelta por la empresa contratista que no reciba el visto bueno de la DSTSC será devuelta a la empresa contratista acumulando los tiempos de resolución.

La DSTSC trabajará juntamente con la empresa contratista para reducir el tiempo de resolución, ya sea proporcionando información, realizando pruebas o a través de cualquier otra acción que esté a su alcance.

5.4. Horario del soporte técnico

El contratista proporcionará un soporte técnico en horario de atención de 9h a 17h, de lunes a viernes, no festivos, en la ciudad de Barcelona.

5.5. Canales de comunicación

La DSTSC utiliza como herramienta de seguimiento de las peticiones el Service Desk de PROLIN. La comunicación de incidencias o peticiones se realizará, a partir de esta herramienta, a la empresa contratista que recibirá un correo electrónico.

Cualquier cambio de situación de la incidencia o petición que realice la empresa contratista debe quedar reflejado en el Service Desk.

En caso de incidencias críticas o urgentes, se utilizará el teléfono en primera instancia, que deberá estar disponible 24x7 y utilizando el catalán o castellano como lengua. Posteriormente, la petición se anotará también en el Service Desk.

Si la empresa contratista utiliza una herramienta propia para la gestión interna de las tareas, se facilitará la integración. Si la integración con la herramienta de la empresa contratista no es posible, la DSTSC proporcionará a un usuario de acceso a su sistema con el único objetivo de garantizar la actualización de los datos. En cualquier caso, la gestión del cumplimiento de ANS correrá a cargo del contratista y no se podrá obtener a partir del sistema de la DSTSC.

5.6. Seguimiento del contrato

El contratista realizará un informe trimestral en relación con la ejecución del contrato, donde figurará la evolución de todas las actuaciones realizadas. Este informe estará a disposición de la DSTSC, antes del 10º día del inicio de cada trimestre posterior, al que se está evaluando.

A continuación, se detalla la información que deberá constar (como mínimo) en este informe de seguimiento del contrato:

Datos del soporte:

- Volumetría servicio:
  - Número de usuarios Microsoft 365 copiados en el período.
  - Restauraciones realizadas.

- Datos de configuración de las copias: retención y periodicidad.

- Gestión de incidencias:
  - Cuadro resumen del período, con el número de incidencias tratadas, agrupadas por categoría y nivel.
  - Situación detallada de las incidencias escaladas. Para cada una de las incidencias el estado, información de la situación, actividades que se están desarrollando para su resolución y planificación de su resolución.
  - Cuadro de cumplimiento de ANS por categoría. El % de cumplimiento se realiza a partir del siguiente algoritmo:

    Total, Incidencias en el ANS / Total incidencias

    Computarán como “total incidencias” las que hayan estado en situación de tratamiento por parte de la contratista en el mes. Computarán como "total incidencias dentro del ANS" el "total incidencias" que estén dentro de los plazos de cumplimiento de los ANS.

    En esta sección se detallarán las incidencias que de acuerdo con la DSTSC, se considere que, por distintos motivos, no deben ser incluidas en este cómputo.

Resumen datos monitorización:

- Tiempo de disponibilidad de la plataforma.
- Alarmas generadas por tipología.
- Datos de la gestión de la capacidad: número usuarios, rendimiento, etc.
- Gráficas de evolución.
- Lista de alarmas acaecidas durante el período.
- Propuestas de evolución de la plataforma.

Datos gestión:

- Estado de acciones de mejora del servicio.
- Situación económica del contrato, indicando las facturas presentadas.

Si los técnicos de la DSTSC lo consideran necesario, se organizarán reuniones de seguimiento, a fin de trabajar para la mejora constante de la prestación. A estas reuniones asistirá por parte de la empresa contratista el responsable del contrato. En estas reuniones se revisarán los informes trimestrales, el funcionamiento de los procesos, se definirán propuestas de mejora y se hará un seguimiento de todo lo relacionado con el contrato. El acta de la reunión correrá a cargo de la empresa contratista.

La DSTSC podrá solicitar informes puntuales sobre problemas, incidencias, cambios, propuestas de mejora, etc. Asimismo, la DSTSC podrá convocar a la empresa contratista por reuniones puntuales sobre temas específicos o reuniones operativas.

En relación con las reuniones a realizar durante el plazo de vigencia del contrato, cualquiera que sea su periodicidad y motivo de su convocatoria, se podrán realizar tanto en modalidad presencial como telemática, siempre a criterio de los técnicos de la DSTSC. La contratista dispondrá de los medios necesarios para adecuarse a cualquiera de los formatos, sin que ello genere coste adicional alguno para la Diputación de Barcelona.

5.7. Equipo de trabajo

En relación con los integrantes del equipo de trabajo que la empresa contratista debe disponer en su plantilla para la prestación del contrato, con independencia de su porcentaje de dedicación final, deberán corresponderse con los siguientes perfiles:

- Responsable del contrato.

  Realizará las labores de coordinación, seguimiento y control de la gestión del contrato. Por parte de la DSTSC se designará a una persona que realizará funciones análogas.

  Será función del responsable del contrato de la empresa contratista conocer en profundidad las prestaciones cubiertas y asegurar que todo el personal de la empresa contratista que participa en el contrato tenga los conocimientos adecuados y asuma los compromisos adquiridos y vele por el cumplimiento de todos los requerimientos incluidos en el contrato.

  Las principales funciones del responsable del contrato son:

  - Coordinación, seguimiento, control de la gestión y calidad del servicio y con quien se trabajará para fijar y revisar la ejecución del contrato. Por parte de la Diputación de Barcelona, la DSTSC designará a un coordinador que realizará las funciones análogas.

  - Supervisión de la puesta en marcha para cumplir con el plan presentado, de acuerdo con los requisitos que determine el coordinador de la DSTSC.

  - Supervisión de los incidentes, problemas, consultas, peticiones, etc.

  - Gestión del escalado. Los incidentes (o cualquier otra acción) que necesiten ser escalados a recursos técnicos oa niveles de responsabilidad superiores

dentro de la propia empresa o en caso de subcontratación a otras empresas, serán gestionados estrechamente para acelerar su resolución.

La empresa contratista deberá estar en disposición de dar cobertura inmediata en caso de enfermedad, vacaciones o cualquier otra contingencia que afecte a su personal, a fin de que en ningún supuesto la prestación quede sin cubrir.

6. Prueba de concepto

La Diputación de Barcelona, a través de la DSTSC, se reserva el derecho a pedir a las empresas licitadoras (inicialmente a la que se haya propuesto como adjudicataria), sin coste adicional, la realización de una prueba de concepto, a fin de validar que la solución tecnológica propuesta se ajusta a las funcionalidades que se han recogido en este pliego de prescripciones técnicas.

La empresa adjudicataria se encargará de preparar en sus instalaciones su producto y facilitar el acceso a los técnicos que determine la DSTSC, de forma que, desde un puesto de trabajo corporativo, que tenga instalada la maqueta estándar corporativa, se pueda realizar dicha comprobación.

Para la realización de la prueba de concepto, los técnicos de la DSTSC proporcionarán a la empresa propuesta como adjudicataria:

- Una dirección IP pública de la Diputación de Barcelona, que debe ser la única dirección IP permitida para acceder al gestor de administración de la herramienta, y desde la que se efectuará esta prueba de concepto.
- Los datos necesarios para que la herramienta de copia de seguridad propuesta pueda conectarse a la plataforma Microsoft 365 de la Diputación de Barcelona para poder efectuar copias de seguridad y restauraciones.
- 3 usuarios del directorio activo de la infraestructura de la Diputación de Barcelona para que puedan acceder a la herramienta, cada uno con los roles que se detallan a continuación.
- 4 usuarios con licencia Microsoft 365 sobre los que se efectuarán las pruebas de copia de seguridad y restauración. Durante la prueba de concepto, se creará un quinto usuario para verificar que es añadido a las políticas de backup de forma automática y desatendida. También, se facilitará un buzón departamental, que deberá copiarse.

Esta prueba se realizará con el apoyo de la DSTSC y con los referentes del Servicio de Gestión de Operaciones TIC, a partir de una validación básica que permita:

1. Validar que el gestor de administración de la herramienta sólo puede accederse desde la dirección IP proporcionada por la Diputación de Barcelona. Se validará que el acceso desde otras direcciones IP a esta página web es denegado y no permite ni siquiera introducir un usuario y contraseña, para evitar intentos de acceso a la fuerza bruta.

2. Validar que el acceso a la herramienta es posible desde los navegadores de la maqueta estándar de la Diputación de Barcelona sin necesidad de instalar ningún complemento o programa que no esté instalado por defecto en la maqueta.

3. Validar que la herramienta permite la validación de los usuarios dados de alta con sus contraseñas del directorio activo. También, se validará el acceso a la herramienta con el usuario local de la misma, según lo especificado en el párrafo 4.2 de los “Requerimientos funcionales”.

4. Asignar a los 3 usuarios creados, los roles de creación de políticas de copias, de recuperación y visualización del log y creación de nuevos usuarios y roles, respectivamente, a fin de validar que cada usuario dispone sólo de sus permisos.

5. Efectuar backup de los datos (buzón de Exchange, datos de Sharepoint, de OneDrive y conversación de Teams) de los 4 usuarios, así como del buzón departamental.

6. Crear en Microsoft 365 un quinto usuario y validar que es añadido a la política de copia de seguridad de forma desatendida, sin acción alguna por parte de los usuarios que efectúan la prueba de concepto, según lo detallado en el presente pliego en el párrafo “Autodescubrimiento de usuarios Microsoft 365”.

7. Configurar copias de seguridad para verificar el punto “Configuración de la planificación y retención”. Efectuar también una copia “on demand”.

8. Una vez efectuadas las copias de seguridad se validará el buscador de documentos.

9. Efectuar una restauración granular de un elemento de un buzón sobre el mismo buzón, sobre otro y en disco. Posteriormente, se eliminará un buzón y se restaurará éste de forma total.

10. Efectuar restauración de un archivo de OneDrive y de elementos de Teams.

11. Una vez efectuadas las validaciones de los puntos anteriores, se comprobará la existencia del log de movimientos y la grabación de los eventos detallados en el presente pliego de las pruebas realizadas anteriormente.

Se considerará que la solución tecnológica propuesta tiene la aceptación de la DSTSC, si se constata que los resultados de la prueba de concepto han permitido garantizar, de forma objetiva, que la solución propuesta ha cumplido con las especificaciones técnicas y los criterios de validación incluidos en la prueba de concepto y detallados en los párrafos precedentes de este mismo apartado.

7. Puesta en marcha

La puesta en marcha es el período de tiempo que transcurre entre el inicio de la ejecución del contrato y la consecución de los niveles de servicio fijados en este Pliego de prescripciones técnicas. En esta fase, el contratista pondrá en marcha los procedimientos y herramientas necesarias para la ejecución del servicio, integrándolos con los procedimientos, procesos y herramientas existentes en la DSTSC.

La DSTSC asignará a un interlocutor que trabajará juntamente con la empresa contratista en la fase de puesta en marcha.

Será responsabilidad del contratista la ejecución de las distintas tareas que conforman la puesta en marcha de la solución.

Durante la primera reunión de trabajo, la empresa contratista deberá presentar el plan de puesta en marcha, que incluirá los mecanismos necesarios para ejecutar toda la puesta en marcha de la solución: traspaso de conocimiento, reuniones, conectividad en el entorno, presentación de recursos asignados y concreción de protocolos de actuación.

Para la puesta en marcha de la solución, la empresa contratista dispondrá de un plazo de ejecución de 30 días naturales o inferior si se mejora en la oferta, a contar a partir de. la fecha de activación de las licencias backup y restore O365. A partir de ese momento, se aplicarán las penalidades correspondientes.

Forman parte de la prestación, actividades, implementación y formación a los usuarios de la corporación, previas a la puesta en marcha para asegurar el correcto funcionamiento del sistema, de acuerdo con las especificaciones detalladas (tanto técnicas como funcionales).

Asimismo, forma parte del proceso de implementación la conexión de la solución de backup a la nube con la infraestructura Microsoft 365 de la Diputación de Barcelona mediante un usuario y contraseña y una primera configuración de las políticas de copias de seguridad según las especificaciones de los técnicos de la DSTSC.

Las copias de seguridad deben empezar a realizarse pasado el plazo de 30 días naturales dedicados a la puesta en marcha de la solución. Una vez configurada la solución y dentro del plazo máximo fijado para su puesta en marcha, la empresa

contratista realizará una formación para traspasar el servicio a los técnicos que la DSTSC indique.

El objetivo de esta formación es que los técnicos de la DSTSC adquieran el conocimiento necesario para que puedan administrar la solución de forma autónoma y hacerla evolucionar según los intereses propios de la DSTSC. La formación consistirá en una jornada de 8 horas y se realizará de forma telemática. En esta formación se deberá traspasar el conocimiento, como mínimo, de los siguientes puntos:

- Acceso a la solución.
- Creación, modificación y eliminación de políticas de copias de seguridad.
- Verificación de las copias de seguridad.
- Realización de copias de seguridad bajo demanda (manualmente).
- Realización de restauraciones de los distintos productos de Microsoft 365.
- Configuración de alertas de backups finalizados, fallidos y no inicializados, así como de eventos de la solución.
- Creación y configuración de usuarios en la solución y aplicación de los diferentes roles.
- Consultas de los logs de registro.

El coste que implique o que se derive de cualquiera de las actuaciones derivadas de la puesta en marcha, debe entenderse incluido en el presupuesto total del contrato.

8. Acuerdos de Nivel de Servicio (ANS)

Los ANS permiten obtener indicadores para la evaluación del grado de cumplimiento del contrato.

El cálculo del ANS se realizará con una periodicidad mensual y considerando el horario de la prestación y el mes natural.

No computarán los períodos de tiempo en que el contratista está pendiente de respuesta, reuniones, datos o concreción de requerimientos por parte de los técnicos o usuarios de la Diputación de Barcelona o de terceros proveedores siempre y cuando éstos no tengan una relación contractual directa con la empresa contratista principal, dado que en ese caso el tiempo computará como tiempo propio del contratista a todos los efectos previstos en este pliego.

8.1. ANS de resolución de incidencias

Las incidencias sólo se considerarán finalizadas si se encuentran completamente documentadas y tienen el visto bueno funcional y técnico de la DSTSC, de lo contrario serán devueltas a la empresa contratista acumulando los tiempos de resolución, a todos los efectos y responsabilidades establecidas en el ANS correspondiente.

Tiempo de respuesta: es el tiempo transcurrido entre la comunicación de la incidencia a la empresa contratista por el canal previsto hasta que ésta la asume asignando los recursos necesarios para poder cumplir el tiempo de resolución.

Tiempo de resolución: es el tiempo transcurrido entre la comunicación de la incidencia a la contratista por el canal previsto, hasta que la incidencia queda resuelta y documentada por la empresa contratista.

Se establecen cuatro categorías de incidencias, con diferentes ANS, por el tiempo de resolución (los tiempos están siempre dentro del horario de servicio, por tanto, siempre computado sobre horas, días o períodos de días naturales):

Indicadores para la gestión de incidencias	Tiempo de resolución
A1. Crítica. Incidencias que suponen no acceder a la solución o afectan de forma muy global a todo el sistema de copias. Incidentes de seguridad nivel Alto.	4 horas
A2. Urgente. Incidencias que suponen el paro de alguna funcionalidad básica.	24 horas
A3. Importante. Incidencias que afectan a una funcionalidad con impacto limitado.	5 días
A4. Estándar. Incidencias que no detienen la operativa diaria.	10 días

8.2. ANS de la disponibilidad del servicio de soporte

La empresa contratista deberá garantizar la disponibilidad del servicio de soporte. En caso de indisponibilidad, el tiempo de resolución será de 2 horas.

9. Transición del servicio

La fase de transición del servicio sólo se activará, en caso de que haya alternancia entre contratistas.

Esta fase de transición del servicio se establece entre el momento en que la nueva empresa se hace cargo del servicio de copias de seguridad y restauraciones y la

expiración de las copias de seguridad de la empresa saliente, con una duración de un año.

Dado el gran volumen de información previsto de las copias de seguridad almacenadas durante la vigencia del contrato, así como por el formato propietario de las copias (que imposibilitarán una posible exportación), y con el objetivo de garantizar la restauración de aquellas copias que no hayan llegado al final de su período de expiración, durante esa fase de transición, la empresa no efectuará más copias y únicamente permitirá restaurar las copias de seguridad existentes en la nube (con la misma granularidad y funcionalidades que en el resto del contrato), mientras que la nueva empresa contratista efectuará copias de seguridad del entorno Microsoft 365 y permitirá la restauración de los nuevos datos durante la vigencia del nuevo contrato.

En este sentido, la empresa contratista deberá comprometerse a realizar una buena gestión y seguimiento de los servicios objeto de este contrato, garantizando su prestación continuada en el tiempo, según los acuerdos de nivel de servicios y con entregas de calidad, así como asegurar el traspaso de información (procedimientos de gestión, datos y documentos) y conocimiento entre contratistas en la fase de transición.

Cuando exista continuidad de contratista ésta deberá entregar a la DSTSC una memoria técnica explicativa proponiendo mejoras, en su caso, en la prestación del servicio.

10. Devolución del servicio

Una vez finalizada la fase de copias y restauraciones, el contratista deberá permitir la descarga de todos los logs de movimientos disponibles en ese momento a la solución. El formato de este log deberá estar en texto plano y con los campos delimitados para poder ser importado a otros aplicativos de análisis, como Excel.

Los objetivos serán:

- Recoger el traspaso de conocimiento por parte del contratista saliente con el fin de garantizar la continuidad del servicio.
- Recogida cuidadosa de requerimientos para la planificación del arranque del servicio por parte del contratista alternativo.
- Preparación y pruebas de los accesos remotos en el sistema de información, para su disponibilidad el día de inicio de la prestación efectiva del servicio.
- Preparación de los entornos necesarios para la adecuada prestación del servicio.

Además, la contratista deberá garantizar, mediante un documento, que ha destruido de forma efectiva, y sin que puedan recuperarse en modo alguno, la totalidad de los datos de las copias de seguridad que estén guardadas en el sistema de almacenamiento en la nube sobre el que ha prestado el servicio durante la vigencia del contrato.

Asimismo, el documento deberá acreditar que la contratista ha desconfigurado e inhabilitado la conexión existente contra la plataforma de Microsoft 365 de la Diputación de Barcelona, de forma que sea imposible acceder a información existente alguna en la

plataforma ni a los usuarios o contraseñas del directorio activo de la Diputación de Barcelona.

11. Transferencia tecnológica y de conocimiento

La contratista está obligada a facilitar a las personas designadas por la DSTSC toda aquella información necesaria para disponer de pleno conocimiento técnico de las prestaciones realizadas.
Asimismo, el personal técnico designado por la DSTSC para realizar gestión de las prestaciones contratadas podrá realizar todas aquellas consultas que considere oportunas para el correcto seguimiento y control del contrato, así como, recibiendo, en su caso, el traspaso de la información que sea necesaria para conocer y comprender el funcionamiento de estos.

DILIGENCIA para hacer constar que el texto que antecede es traducción al castellano del Pliego de Prescripciones Técnicas Particulares, aprobado por Decreto de fecha 27/05/2026. En caso de discrepancia entre dicho Pliego, en catalán, y esta traducción al castellano, prevalecerá el primero.

Metadades del document

Núm. expedient	2026/0004487
Tipus documental	Plec de clàusules o condicions
Títol	Pliego de prescripciones técnicas particulares para la contratación de una solución integral de gestión de la copia de seguridad y restauración, en la nube, de la plataforma Microsoft 365 de la Diputación 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	29/05/2026, 09:09

Validació Electrònica del document

Codi (CSV)	Adreça de validació	QR
a25fd920f80dbbf60e06	https://seuelectronica.diba.cat	